| | |
|---|---|
| **Tab 1** | **SB 7098** by **GO**; (Compare to H 07105) Death Benefits |

| | |
|---|---|
| **Tab 2** | **SB 1570** by **Hooper**; (Identical to H 05301) Information Technology Reorganization |

**The Florida Senate**

# COMMITTEE MEETING EXPANDED AGENDA

**APPROPRIATIONS SUBCOMMITTEE ON AGRICULTURE, ENVIRONMENT AND GENERAL GOVERNMENT**
**Senator Mayfield, Chair**
**Senator Powell, Vice Chair**

**MEETING DATE:** Tuesday, April 16, 2019
**TIME:** 9:00 a.m.—12:00 noon
**PLACE:** *Toni Jennings Committee Room,* 110 Senate Building

**MEMBERS:** Senator Mayfield, Chair; Senator Powell, Vice Chair; Senators Albritton, Bean, Berman, Broxson, Hooper, Hutson, Rodriguez, and Stewart

| TAB | BILL NO. and INTRODUCER | BILL DESCRIPTION and SENATE COMMITTEE ACTIONS | COMMITTEE ACTION |
|---|---|---|---|
| 1 | **SB 7098**<br>Governmental Oversight and Accountability<br>(Compare H 7105, S 1548) | Death Benefits; Amending provisions relating to death benefits for law enforcement, correctional, and correctional probation officers and for firefighters, respectively; revising the payment amounts of death benefits; establishing a death benefit for emergency medical technicians and paramedics to conform to s. 31, Art. X of the State Constitution; specifying eligibility and payment amounts for such death benefits, etc.<br><br>AEG 04/16/2019 Favorable<br>AP | Favorable<br>Yeas 9 Nays 0 |
| 2 | **SB 1570**<br>Hooper<br>(Identical H 5301, Compare S 2502) | Information Technology Reorganization; Transferring all powers, duties, functions, records, offices, personnel, associated administrative support positions, property, pending issues and existing contracts, administrative authority, certain administrative rules, trust funds, and unexpended balances of appropriations, allocations, and other funds of the Agency for State Technology to the Department of Management Services by a type two transfer; requiring each state agency to adopt formal procedures for cloud-computing options, etc.<br><br>GO 03/26/2019 Favorable<br>AEG 04/16/2019 Favorable<br>AP | Favorable<br>Yeas 10 Nays 0 |
| 3 | Presentation on Environmental Needs of North Florida by Honorable Steve Southerland, Chairman, Stand up for North Florida | | Presented |

Other Related Meeting Documents

**The Florida Senate**

# BILL ANALYSIS AND FISCAL IMPACT STATEMENT

(This document is based on the provisions contained in the legislation as of the latest date listed below.)

| Prepared By: The Professional Staff of the Appropriations Subcommittee on Agriculture, Environment, and General Government | |
|---|---|
| BILL: | SB 7098 |
| INTRODUCER: | Governmental Oversight and Accountability Committee |
| SUBJECT: | Death Benefits |
| DATE: | April 15, 2019 |
| REVISED: | |

| | ANALYST | STAFF DIRECTOR | REFERENCE | ACTION |
|---|---|---|---|---|
| | McVaney | McVaney | | **GO Submitted as Committee Bill** |
| 1. | McSwain/Shettle | Betta | AEG | **Recommend: Favorable** |
| 2. | | | AP | |

## I. Summary:


SB 7098 implements Amendment 7 to the State Constitution, which was approved by the voters in November 2018 to require the payment of death benefits to the survivors of certain first responders, Florida National Guard members, and members of the United States Armed Forces. Current law provides various death benefits to many, but not all, of the first responders, Florida National Guard members, and members of the U.S. Armed Forces who are eligible for benefits under Amendment 7. Therefore, the Legislature must expand some of the current death benefits to comply with the requirements of Amendment 7.

The bill expands the death benefits currently provided to Florida National Guard members on state active duty, firefighters, and law enforcement, correctional, and correctional probation officers and sets the amount of the benefits as follows:

- $75,000 when an eligible firefighter, Florida National Guard member, or law enforcement, correctional, or correctional probation officer is accidentally killed or receives accidental bodily injury that results in the loss of the individual's life.
- An additional $75,000 when an eligible firefighter or law enforcement, correctional, or correctional probation officer is accidentally killed in the above manner and meets additional requirements, such as the accidental death occurs as a result of the response to an emergency.
- $225,000 when an eligible firefighter, Florida National Guard member, or law enforcement, correctional, or correctional probation officer is unlawfully and intentionally killed or dies as a result of an unlawful and intentional act while engaged in the performance of official duties.

The bill also provides the benefits described above to paramedics and emergency medical technicians.

The bill removes the annual Consumer Price Index adjustment of the benefit amounts.

The bill creates a new death benefit of $75,000 for members of the U.S. Armed Forces, including Florida National Guard members, who are killed while on federal active duty and engaged in performing official duties. Other members of the U.S. Armed Forces who are killed while on active duty but not engaged in the performance of their official duties are entitled to a $25,000 death benefit.

The bill expands death benefits for certain educational expenses of surviving spouses and children by providing them to firefighters, law enforcement officers, correctional officers, correctional probation officers, and Florida National Guard members who are accidentally killed or receive accidental bodily injury resulting in loss of life. These benefits for educational expenses are also provided to paramedics and emergency medical technicians, as well as Florida National Guard members who are killed while on federal active duty and U.S. Armed Forces members who are killed while on active duty.

The bill appears to have an indeterminate fiscal impact on the state and local governments. The proposed bill includes a continuing appropriation from the General Revenue Fund to pay for any monetary benefits related to deceased members of the U.S. Armed Forces.

The bill takes effect July 1, 2019.

## II. Present Situation:

**Constitutional Requirements**

Amendment 7 created Article X, s. 31 of the State Constitution to require a death benefit to be paid by the employing agency and the state to waive certain education expenses when a law enforcement officer, correctional officer, correctional probation officer, firefighter, paramedic, emergency medical technician or a member of the Florida National Guard, while engaged in the performance of official duties, is killed accidentally, unlawfully and intentionally, or during active duty. The surviving child or children and spouse are eligible to benefit from the waiver of educational expenses while obtaining a career certificate, an undergraduate education, or a postgraduate education.

In addition, the State Constitution requires a death benefit to be paid from the General Revenue Fund and the state to waive certain education expenses when a member of the United States Armed Forces, including a Florida National Guard member on federal active duty, is killed accidentally, unlawfully and intentionally, or during active duty. The surviving child or children and spouse are eligible to benefit from the waiver of educational expenses while obtaining a career certificate, an undergraduate education, or a postgraduate education.

To be eligible for the benefits under the State Constitution, the law enforcement officer, correctional officer, correctional probation officer, firefighter, paramedic, and emergency medical technician must be employed by the state or any of its subdivisions at the time of death. For a member of the military to be eligible, the member must have been a resident of the state or his or her duty post must have been within the state, at the time of death.

The constitutional provision takes effect July 1, 2019.

**Statutorily-Authorized Death Benefits**

State law provides a variety of death benefits for public employees. The current statutory benefits may be associated with supplemental benefits provided under chapter 112, F.S., death benefits provided under state and local government retirement systems, emergency responder death benefits administered by the Department of Legal Affairs, and workers compensation.

**Supplemental Benefits Under Chapter 112, Florida Statutes**

***Law Enforcement Officers, Correctional Officers, Correctional Probation Officers, and Firefighters***

Sections 112.19 and 112.191, F.S., provide death benefits, including a monetary payment, waiver of educational costs, and health insurance premiums, to surviving family members of law enforcement officers, correctional officers, correctional probation officers, and firefighters killed under certain circumstances.

In 2002, the monetary payment was adjusted statutorily to $50,000 and has been adjusted annually by the growth in the Consumer Price Index. The benefit for law enforcement officers, correctional officers, and correctional probation officers is set by rules adopted by the Department of Legal Affairs. The benefit for firefighters is set by rules adopted the Department of Financial Services. The benefits for Fiscal Year 2018-2019[1] are shown in the table below.

| Fiscal Year | Department of Legal Affairs | | | Department of Financial Services | | |
|---|---|---|---|---|---|---|
| | Accident | Enhanced Accident | Intentional/ Unlawful | Accident | Enhanced Accident | Intentional/ Unlawful |
| **2018-19** | $65,641.62 | $65,641.62 | $197,875.61 | $69,801.94 | $69,801.94 | $194,470.19 |

The educational benefits are provided to the following public employees:

- A law enforcement officer, correctional officer, and correctional probation officer killed accidentally or as a result of accidental injuries and the accidental death occurs:
  - As a result of the officer's response to fresh pursuit;
  - As a result of the officer's response to what is reasonably believed to be an emergency;
  - At the scene of a traffic accident to which the officer has responded; or
  - While the officer is enforcing what is reasonably believed to be a traffic law or ordinance.
- A firefighter killed accidentally or as a result of accidental injuries and the accidental death occurs:
  - As a result of the firefighter's response to what is reasonably believed to be an emergency involving the protection of life or property; or
  - As a result of the firefighter's participation in a training exercise.
- A law enforcement officer, correctional officer, correctional probation officer, or firefighter who is unlawfully and intentionally killed or is injured by an unlawful and intentional act of another person and dies as a result of the injury.

[1] Rules 2A-8.005 and 69A-64.005, Florida Administrative Code.

The educational benefit is granted to the surviving children and spouse of the deceased employee. This benefit is a waiver, by the state educational institution, of the tuition and fees associated with attaining a career certificate, an undergraduate education, or a postgraduate education. An eligible child may use the waiver until the child's 25th birthday. An eligible spouse may use the waiver until the 10th anniversary of the employee's death.

***Florida National Guard***

Section 250.34(4), F.S., provides that a Florida National Guard member who is killed or who dies due to injuries received while on active state duty qualifies for the same benefits provided to law enforcement officers under s. 112.19, F.S. However, when the federal government activates a Florida National Guard member for active duty and the member dies in the line of duty while on active federal duty, the death benefit is determined by federal law and is paid by the federal government. There are no state benefits provided if the member dies while on federal active duty.

**Death Benefits for U.S. Armed Forces Members**

Survivors of active duty members of the U.S. Armed Forces receive certain payments or benefits regardless of whether the in-service death is due to combat, accident, or disease, including:[2]

- Burial benefits, which may include a gravesite in any VA national cemetery with available space, perpetual care of the grave at no cost to the family, a government headstone or marker, Presidential Memorial Certificate, and a U.S. burial flag;
- Dependency and indemnity compensation for a surviving spouse and dependent children; and
- Life insurance.

Florida provides postsecondary scholarships for dependent children and surviving spouses who have not remarried and meet certain eligibility requirements, including requirements that the deceased service member was a resident of the state for one year immediately preceding the death and that the spouse applied for benefits within five years after the service member's death. The scholarships are distributed on a first-come, first-served basis by the Department of Education and are funded by general revenue. None of the other benefits provided for members of the U.S. Armed Forces are paid from general revenue.

**Florida Retirement System Death Benefits**

The Florida Retirement System (FRS) provides death benefits for members who are killed in the line of duty.[3] Employers participating in the FRS include state agencies, counties, cities, special districts, school boards, and state universities and colleges. The surviving spouse of a member killed in the line of duty may receive a monthly pension equal to one-half of the monthly salary being received by the member at the time of death for the rest of the spouse's life, or, if the member had a vested retirement benefit, the spouse could elect to receive the member's

[2] Off. Pub. Aff. Media Rel., Deaths on Active Duty – Survivor Benefits, DEP'T VETERANS AFF., Jan. 2009, available at https://www.va.gov/opa/publications/factsheets/fs_survivor_benefits.pdf; U.S. Dep't. of Veterans Aff., Veterans Benefits Administration – Dependents and Survivors' Benefits, DEP'T VETERANS AFF., Oct. 2018, available at https://benefits.va.gov/benefits/factsheets.asp#BM6 (last visited March 30, 2019).
[3] Sections 121.091(7), and 121.591(4), F.S.

retirement benefit.[4] If the member was not married, benefits are paid to the surviving children.[5] If the member dies in the line of duty and was a member of the Special Risk Class,[6] which includes firefighters, law enforcement officers, correctional officers, correctional probation officers, paramedics and emergency medical technicians, the surviving spouse or children are entitled to an additional one-half of the member's monthly salary.[7] As such, the death benefit provided under the FRS for those members equals 100 percent of the member's salary.

**Emergency Responder Death Benefits**

Section 960.194, F.S., allows the Department of Legal Affairs to award up to $50,000 to the surviving family members of a law enforcement officer, firefighter, paramedic, or emergency medical technician who, as a result of a crime, is killed answering a call for service in the line of duty.

## III. Effect of Proposed Changes:

**Section 1** reenacts and amends s. 112.19, F.S., to set the level of death benefits for law enforcement officers, correctional officers, and correctional probation officers. If the officer, while engaged in the performance of the officer's official duties, is accidentally killed or receives an accidental bodily injury which results in death, the death benefit is $75,000. If the officer is accidentally killed under certain circumstances, an additional death benefit of $75,000 is payable. If the officer, while engaged in the performance of the officer's official duties, is unlawfully and intentionally killed or dies as a result of an unlawful and intentional act, the death benefit is $225,000. Because the statutorily-authorized death benefit amounts are no longer adjustable, the rulemaking authority of the Department of Legal Affairs is eliminated. The death benefits continue to be payable by the employer the same way such benefits are payable under current law. All monetary death benefits established in this section are payable by the employer, including the state, cities, counties, universities, colleges, school boards, and special districts.

Section 1 continues the education benefits currently afforded to survivors of law enforcement officers, correctional officers and correctional probation officers killed prior to July 1, 2019.

**Section 2** reenacts and amends s. 112.191, F.S., to set the level of death benefits for firefighters. The benefits are expanded to include part-time firefighters. If the firefighter, while in the performance of the firefighter's official duties, is accidentally killed or receives an accidental bodily injury which results in death, the death benefit is $75,000. If the firefighter is accidentally killed under certain circumstances, an additional death benefit of $75,000 is payable. If the firefighter, while in the performance of the firefighter's official duties, is unlawfully and intentionally killed or dies as a result of an unlawful and intentional act, the death benefit is $225,000. Because the statutorily-authorized death benefit amounts are no longer adjustable, the rulemaking authority of the Bureau of Crime Prevention and Training is eliminated. The death benefits continue to be payable by the employer the same way such benefits are payable under

[4] Section 121.091(7)(d)1., F.S.
[5] Section 121.091(7)(d)3., F.S.
[6] Section 121.0515, F.S.
[7] Section 121.091(7)(i), F.S.

current law. All monetary death benefits established in this section are payable by the employer, including the state, cities, counties, universities, colleges, school boards, and special districts.

Section 2 continues the education benefits currently afforded to survivors of firefighters killed prior to July 1, 2019.

**Section 3** creates s. 112.1911, F.S., to set the level of death benefits for paramedics and emergency medical technicians (EMT). If the paramedic or EMT, while in the performance of official duties, is accidentally killed or receives an accidental bodily injury which results in death, the death benefit is $75,000. If the paramedic or EMT is accidentally killed under certain circumstances, an additional death benefit of $75,000 is payable. If the paramedic or EMT, while in the performance of official duties, is unlawfully and intentionally killed or dies as a result of an unlawful and intentional act, the death benefit is $225,000. The death benefits are payable by the employer. All monetary death benefits established in this section are payable by the employer, including the state, cities, counties, universities, colleges, school boards, and special districts.

**Section 4** creates s. 112.1912, F.S., to establish educational benefits for children and spouses of first responders killed in the line of duty on or after July 1, 2019. The benefits are similar to the benefits currently provided under ss. 112.19 and 112.191, F.S. However, the eligibility for benefits is expanded to include any first responders accidentally killed while engaged in the performance of their official duties and paramedics and EMTs killed while engaged in the performance of their duties. The educational benefits established in this section are funded through waivers by the educational institutions attended by the eligible survivors.

**Section 5** amends s. 250.34, F.S., to establish a $75,000 death benefit for a member of the Florida National Guard who is killed accidentally or receives accidental bodily injury resulting in death, while on state active duty and engaged in official duties. A death benefit of $225,000 is granted if the member is killed unlawfully and intentionally while on state active duty and engaged in official duties. The section also makes the survivors of the members of the Florida National Guard killed in these circumstances eligible for the educational benefits provided in s. 112.1912, F.S., created by section 4 of this bill. The monetary benefits established by this section are payable by the state.

**Section 6** reenacts and amends s. 295.01, F.S., to clarify that a person using benefits under this provision is not eligible to use benefits under s. 295.061, F.S., created in section 7 of this act. The eligible child or spouse is permitted to elect to use either the scholarship or the waiver of tuition and fees to seek education benefits.

**Section 7** creates s. 295.061, F.S., to provide death benefits to members of the U.S. Armed Forces who are either residents of the State of Florida or whose duty station is located in Florida. If the service member is killed while on active duty and engaged in official duties, the death benefit is $75,000, payable by the state. If the service member is killed while on active duty but under other circumstances, the death benefit is $25,000, payable by the state.

This section also established an educational benefit for survivors of service members killed while on active duty. The benefits are mirror the benefits provided pursuant to s. 112.1912, F.S., created in section 4 of this bill.

**Section 8** provides that the bill takes effect July 1, 2019.

## IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

Not applicable. This bill implements constitutional provisions requiring government entities to pay death benefits for certain first responders employed by government entities and killed while engaged in the performance of their official duties.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

D. State Tax or Fee Increases:

None.

E. Other Constitutional Issues:

None identified.

## V. Fiscal Impact Statement:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

None.

C. Government Sector Impact:

The overall impact on state and local government expenditures is indeterminate.

The state and local governments may incur additional costs for the monetary death benefits granted to the surviving family members of first responders killed while engaged in the performance of their official duties. These benefits are paid by the employers of the employee.

The state may incur additional costs for the monetary death benefits granted to the surviving family members of a member of the U.S. Armed Forces killed while on active duty. These benefits are paid from the General Revenue Fund.

State universities and colleges will forego tuition and fee revenues associated with the waivers granted by the state to children and spouses of emergency medical technicians, paramedics, and eligible members of the U.S. Armed Forces killed while on active duty.

## VI. Technical Deficiencies:

None.

## VII. Related Issues:

None.

## VIII. Statutes Affected:

This bill substantially amends the following sections of the Florida Statutes: 112.19, 112.191, 250.34, and 295.01.

This bill creates the following sections of the Florida Statutes: 112.1911, 112.1912, and 295.061.

## IX. Additional Information:

A. Committee Substitute – Statement of Changes:
(Summarizing differences between the Committee Substitute and the prior version of the bill.)

None.

B. Amendments:

None.

This Senate Bill Analysis does not reflect the intent or official position of the bill's introducer or the Florida Senate.

**By** the Committee on Governmental Oversight and Accountability

585-03750-19 20197098__

A bill to be entitled

An act relating to death benefits; reenacting and amending ss. 112.19 and 112.191, F.S., relating to death benefits for law enforcement, correctional, and correctional probation officers and for firefighters, respectively; revising definitions; revising the payment amounts of death benefits; deleting the provision requiring annual adjustment of the death benefit amount; conforming provisions regarding the waiver for specified educational expenses to changes made by the act; creating s. 112.1911, F.S.; establishing a death benefit for emergency medical technicians and paramedics to conform to s. 31, Art. X of the State Constitution; providing definitions; specifying eligibility and payment amounts for such death benefits; prescribing the procedure by which an emergency medical technician or a paramedic designates a beneficiary; specifying that such death benefits are supplementary and exempt from creditors' demands or claims; specifying the financial responsibility of employing agencies as to the payment of benefits; creating s. 112.1912, F.S.; defining the term "first responder"; providing a death benefit for certain educational expenses for the surviving spouse and children of certain first responders; authorizing a specified number of hours to be waived by certain educational institutions; providing requirements to receive such benefit; requiring the State Board of Education and the Board of Governors to adopt rules



**CODING:** Words ~~stricken~~ are deletions; words underlined are additions.



585-03750-19 20197098__

and regulations, respectively; amending s. 250.34, F.S.; modifying eligibility for certain death benefits for a deceased member of the Florida National Guard, to conform to s. 31, Art. X of the State Constitution; prescribing the procedure by which a Florida National Guard member designates a beneficiary; specifying that such death benefits are exempt from creditors' claims and demands; specifying eligibility for educational benefits for the member's surviving children and spouse; reenacting and amending s. 295.01, F.S.; modifying provisions governing educational expense waivers for the child or spouse of a servicemember; creating s. 295.061, F.S.; providing definitions; establishing a death benefit for active duty members of the United States Armed Forces, to conform to s. 31, Art. X of the State Constitution; specifying eligibility and other requirements for entitlement to such benefits; specifying the payment amount of such benefits; prescribing the procedure by which an active duty member designates a beneficiary; specifying that the state-funded benefit is in addition to any federal benefit; providing for funding of the death benefit; requiring the state to waive certain educational expenses of a child or spouse of a deceased active duty member of the United States Armed Forces; specifying conditions and requirements for the waiver; authorizing the State Board of Education and the Board of Governors to adopt rules and regulations, respectively; providing an effective date.



**CODING:** Words ~~stricken~~ are deletions; words underlined are additions.

Be It Enacted by the Legislature of the State of Florida:

Section 1. Section 112.19, Florida Statutes, is reenacted and amended to read:

112.19 Law enforcement, correctional, and correctional probation officers; death benefits.—

(1) As ~~Whenever~~ used in this section, the term:

(a) "Employer" means a state board, commission, department, division, bureau, or agency, or a county, municipality, or other political subdivision of the state, which employs, appoints, or otherwise engages the services of law enforcement, correctional, or correctional probation officers.

(b) "Law enforcement, correctional, or correctional probation officer" means any officer as defined in s. 943.10(14) or employee of the state or any political subdivision of the state, including any law enforcement officer, correctional officer, correctional probation officer, state attorney investigator, or public defender investigator, whose duties require such officer or employee to investigate, pursue, apprehend, arrest, transport, or maintain custody of persons who are charged with, suspected of committing, or convicted of a crime; and the term includes any member of a bomb disposal unit whose primary responsibility is the location, handling, and disposal of explosive devices. The term also includes any full-time officer or employee of the state or any political subdivision of the state, certified pursuant to chapter 943, whose duties require such officer to serve process or to attend a session of a circuit or county court as bailiff.





(c) "Insurance" means insurance procured from a stock company or mutual company or association or exchange authorized to do business as an insurer in this state.

(d) "Fresh pursuit" means the pursuit of a person who has committed or is reasonably suspected of having committed a felony, misdemeanor, traffic infraction, or violation of a county or municipal ordinance. The term does not imply instant pursuit, but pursuit without unreasonable delay.

(2)(a) The sum of $75,000 must ~~$50,000, as adjusted pursuant to paragraph (j), shall~~ be paid as provided in this section when a law enforcement, correctional, or correctional probation officer, while engaged in the performance of the officer's law enforcement duties, is accidentally killed or receives accidental bodily injury which results in the loss of the officer's life, provided that such killing is not the result of suicide and that such bodily injury is not intentionally self-inflicted. ~~Notwithstanding any other provision of law, in no case shall the amount payable under this subsection be less than the actual amount stated therein.~~

(b) The sum of $75,000 must ~~$50,000, as adjusted under paragraph (j), shall~~ be paid as provided in this section if a law enforcement, correctional, or correctional probation officer is accidentally killed as specified in paragraph (a) and the accidental death occurs:

1. As a result of the officer's response to fresh pursuit;

2. As a result of the officer's response to what is reasonably believed to be an emergency;

3. At the scene of a traffic accident to which the officer has responded; or

4. While the officer is enforcing what is reasonably believed to be a traffic law or ordinance.

This sum is in addition to any sum provided for in paragraph (a). ~~Notwithstanding any other provision of law, in no case shall the amount payable under this subsection be less than the actual amount stated therein.~~

(c) If a law enforcement, correctional, or correctional probation officer, while engaged in the performance of the officer's law enforcement duties, is unlawfully and intentionally killed or dies as a result of such unlawful and intentional act, the sum of $225,000 must ~~$150,000, as adjusted pursuant to paragraph (j), shall~~ be paid as provided in this section. ~~Notwithstanding any other provision of law, in no case shall the amount payable under this subsection be less than the actual amount stated therein.~~

(d) Such payments, pursuant to ~~the provisions of~~ paragraphs (a), (b), and (c), whether secured by insurance or not, must ~~shall~~ be made to the beneficiary designated by such law enforcement, correctional, or correctional probation officer in writing, signed by the officer and delivered to the employer during the officer's lifetime. If no such designation is made, then the payments must ~~it shall~~ be paid to the officer's surviving child or children and to the officer's surviving spouse in equal portions, and if there is no surviving child or spouse, then to the officer's parent or parents. If a beneficiary is not designated and there is no surviving child, spouse, or parent, then the sum must ~~it shall~~ be paid to the officer's estate.





(e) Such payments, pursuant to ~~the provisions of~~ paragraphs (a), (b), and (c), are in addition to any workers' compensation or retirement plan ~~pension~~ benefits and are exempt from the claims and demands of creditors of such law enforcement, correctional, or correctional probation officer.

(f) If a full-time law enforcement, correctional, or correctional probation officer who is certified pursuant to chapter 943 and employed by a state agency is killed in the line of duty while the officer is engaged in the performance of law enforcement duties or as a result of an assault against the officer under riot conditions:

1. The sum of $1,000 must ~~shall~~ be paid, as provided for in paragraph (d), toward the funeral and burial expenses of such officer. Such benefits are in addition to any other benefits to which employee beneficiaries and dependents are entitled under the Workers' Compensation Law or any other state or federal statutes; and

2. The officer's employing agency may pay up to $5,000 directly toward the venue expenses associated with the funeral and burial services of such officer.

(g) Any political subdivision of the state that employs a full-time law enforcement officer as defined in s. 943.10(1) or a full-time correctional officer as defined in s. 943.10(2) who is killed in the line of duty on or after July 1, 1993, as a result of an act of violence inflicted by another person while the officer is engaged in the performance of law enforcement duties or as a result of an assault against the officer under riot conditions shall pay the entire premium of the political subdivision's health insurance plan for the employee's surviving

spouse until remarried, and for each dependent child of the employee until the child reaches the age of majority or until the end of the calendar year in which the child reaches the age of 25 if:

1. At the time of the employee's death, the child is dependent upon the employee for support; and

2. The surviving child continues to be dependent for support, or the surviving child is a full-time or part-time student and is dependent for support.

(h)1. Any employer who employs a full-time law enforcement, correctional, or correctional probation officer who, on or after January 1, 1995, suffers a catastrophic injury, as defined in s. 440.02, Florida Statutes 2002, in the line of duty shall pay the entire premium of the employer's health insurance plan for the injured employee, the injured employee's spouse, and for each dependent child of the injured employee until the child reaches the age of majority or until the end of the calendar year in which the child reaches the age of 25 if the child continues to be dependent for support, or the child is a full-time or part-time student and is dependent for support. The term "health insurance plan" does not include supplemental benefits that are not part of the basic group health insurance plan. If the injured employee subsequently dies, the employer shall continue to pay the entire health insurance premium for the surviving spouse until remarried, and for the dependent children, under the conditions outlined in this paragraph. However:

a. Health insurance benefits payable from any other source shall reduce benefits payable under this section.

b. It is unlawful for a person to willfully and knowingly





make, or cause to be made, or to assist, conspire with, or urge another to make, or cause to be made, any false, fraudulent, or misleading oral or written statement to obtain health insurance coverage as provided under this paragraph. A person who violates this sub-subparagraph commits a misdemeanor of the first degree, punishable as provided in s. 775.082 or s. 775.083.

c. In addition to any applicable criminal penalty, upon conviction for a violation as described in sub-subparagraph b., a law enforcement, correctional, or correctional probation officer or other beneficiary who receives or seeks to receive health insurance benefits under this paragraph shall forfeit the right to receive such health insurance benefits, and shall reimburse the employer for all benefits paid due to the fraud or other prohibited activity. For purposes of this sub-subparagraph, the term "conviction" means a determination of guilt that is the result of a plea or trial, regardless of whether adjudication is withheld.

2. In order for the officer, spouse, and dependent children to be eligible for such insurance coverage, the injury must have occurred as the result of the officer's response to fresh pursuit, the officer's response to what is reasonably believed to be an emergency, or an unlawful act perpetrated by another. Except as otherwise provided herein, ~~nothing in~~ this paragraph may not ~~shall~~ be construed to limit health insurance coverage for which the officer, spouse, or dependent children may otherwise be eligible, except that a person who qualifies under this section is ~~shall~~ not ~~be~~ eligible for the health insurance subsidy provided under chapter 121, chapter 175, or chapter 185.

(i) The Bureau of Crime Prevention and Training within the

Department of Legal Affairs shall adopt rules necessary to implement paragraphs (a), (b), and (c).

~~(j) Any payments made pursuant to paragraph (a), paragraph (b), or paragraph (c) shall consist of the statutory amount adjusted to reflect price level changes since the effective date of this act. The Bureau of Crime Prevention and Training shall by rule adjust the statutory amount based on the Consumer Price Index for All Urban Consumers published by the United States Department of Labor. Adjustment shall be made July 1 of each year using the most recent month for which data are available at the time of the adjustment.~~

(3) If a law enforcement, correctional, or correctional probation officer is accidentally killed as specified in paragraph (2)(b) on or after June 22, 1990, but before July 1, 2019, or unlawfully and intentionally killed as specified in paragraph (2)(c) on or after July 1, 1980, but before July 1, 2019, the state must ~~shall~~ waive certain educational expenses that the child or spouse of the deceased officer incurs while obtaining a career certificate, an undergraduate education, or a postgraduate education. The amount waived by the state must ~~shall~~ be in an amount equal to the cost of tuition and matriculation and registration fees for a total of 120 credit hours. The child or spouse may attend a state career center, a Florida College System institution, or a state university~~. The child or spouse may attend any or all of the institutions specified in this subsection,~~ on either a full-time or part-time basis. The benefits provided to a child under this subsection shall continue until the child's 25th birthday. The benefits provided to a spouse under this subsection must commence within





5 years after the death occurs, and entitlement thereto shall continue until the 10th anniversary of that death.

(a) Upon failure of any child or spouse who receives a waiver in accordance with ~~benefited by the provisions of~~ this subsection to comply with the ordinary and minimum requirements regarding discipline and scholarship of the institution attended, such ~~both as to discipline and scholarship, the~~ benefits must ~~shall~~ be withdrawn as to the child or spouse and no further moneys may be expended for the child's or spouse's benefits so long as such failure or delinquency continues.

(b) Only a student in good standing in his or her respective institution may receive the benefits provided in this subsection ~~thereof~~.

(c) A child or spouse receiving benefits under this subsection must be enrolled according to the customary rules and requirements of the institution attended.

(4)(a) The employer of such law enforcement, correctional, or correctional probation officer is liable for the payment of the sums specified in this section and is deemed self-insured, unless it procures and maintains, or has already procured and maintained, insurance to secure such payments. Any such insurance may cover only the risks indicated in this section, in the amounts indicated in this section, or it may cover those risks and additional risks and may be in larger amounts. Any such insurance must ~~shall~~ be placed by such employer only after public bid of such insurance coverage which must ~~coverage shall~~ be awarded to the carrier making the lowest best bid.

(b) Payment of benefits to beneficiaries of state employees, or of the premiums to cover the risk, under ~~the~~

~~provisions of~~ this section must ~~shall~~ be paid from existing funds otherwise appropriated to the department employing the law enforcement, correctional, or correctional probation officers.

(5) The State Board of Education shall adopt rules and procedures, and the Board of Governors shall adopt regulations and procedures, as are appropriate and necessary to implement the educational benefits provisions of this section.

(6) Notwithstanding any provision of this section to the contrary, the death benefits provided in paragraphs (2)(c) and (g) shall also be applicable and paid in cases where an officer received bodily injury before ~~prior to~~ July 1, 1993, and subsequently died on or after July 1, 1993, as a result of such in-line-of-duty injury attributable to an unlawful and intentional act, or an act of violence inflicted by another, or an assault on the officer under riot conditions. Payment of such benefits must ~~shall~~ be in accordance with ~~provisions of~~ this section. ~~Nothing in~~ This subsection may not ~~provision shall~~ be construed to limit death benefits for which those individuals listed in paragraph (2)(d) may otherwise be eligible.

Section 2. Section 112.191, Florida Statutes, is reenacted and amended to read:

112.191 Firefighters; death benefits.—

(1) As ~~Whenever~~ used in this section, the term ~~act~~:

(a) ~~The term~~ "Employer" means a state board, commission, department, division, bureau, or agency, or a county, municipality, or other political subdivision of the state.

(b) ~~The term~~ "Firefighter" means any ~~full-time~~ duly employed uniformed firefighter employed by an employer, whose primary duty is the prevention and extinguishing of fires, the





protection of life and property therefrom, the enforcement of municipal, county, and state fire prevention codes, as well as the enforcement of any law pertaining to the prevention and control of fires, who is certified pursuant to s. 633.408 and who is a member of a duly constituted fire department of such employer or who is a volunteer firefighter.

(c) ~~The term~~ "Insurance" means insurance procured from a stock company or mutual company or association or exchange authorized to do business as an insurer in this state.

(2)(a) The sum of $75,000 must ~~$50,000, as adjusted pursuant to paragraph (i), shall~~ be paid as provided in this section when a firefighter, while engaged in the performance of his or her firefighter duties, is accidentally killed or receives accidental bodily injury which subsequently results in the loss of the firefighter's life, provided that such killing is not the result of suicide and that such bodily injury is not intentionally self-inflicted. ~~Notwithstanding any other provision of law, in no case shall the amount payable under this subsection be less than the actual amount stated therein.~~

(b) The sum of $75,000 must ~~$50,000, as adjusted pursuant to paragraph (i), shall~~ be paid as provided in this section if a firefighter is accidentally killed as specified in paragraph (a) and the accidental death occurs as a result of the firefighter's response to what is reasonably believed to be an emergency involving the protection of life or property or the firefighter's participation in a training exercise. This sum is in addition to any sum provided in paragraph (a). ~~Notwithstanding any other provision of law, the amount payable under this subsection may not be less than the actual amount~~

~~stated therein.~~

(c) If a firefighter, while engaged in the performance of his or her firefighter duties, is unlawfully and intentionally killed, is injured by an unlawful and intentional act of another person and dies as a result of such injury, dies as a result of a fire which has been determined to have been caused by an act of arson, or subsequently dies as a result of injuries sustained therefrom, the sum of $225,000 must ~~$150,000, as adjusted pursuant to paragraph (i), shall~~ be paid as provided in this section. ~~Notwithstanding any other provision of law, the amount payable under this subsection may not be less than the actual amount stated therein.~~

(d) Such payments, pursuant to paragraphs (a), (b), and (c), whether secured by insurance or not, must ~~shall~~ be made to the beneficiary designated by such firefighter in writing, signed by the firefighter and delivered to the employer during the firefighter's lifetime. If no such designation is made, then the payment must ~~it shall~~ be paid to the firefighter's surviving child or children and to the firefighter's surviving spouse in equal portions, and if there be no surviving child or spouse, then to the firefighter's parent or parents. If a beneficiary designation is not made and there is no surviving child, spouse, or parent, then the sum must ~~it shall~~ be paid to the firefighter's estate.

(e) Such payments, pursuant to ~~the provisions of~~ paragraphs (a), (b), and (c), are ~~shall be~~ in addition to any workers' compensation or retirement plan ~~pension~~ benefits and are ~~shall be~~ exempt from the claims and demands of creditors of such firefighter.





(f) Any political subdivision of the state that employs a full-time firefighter who is killed in the line of duty on or after July 1, 1993, as a result of an act of violence inflicted by another person while the firefighter is engaged in the performance of firefighter duties, as a result of a fire which has been determined to have been caused by an act of arson, or as a result of an assault against the firefighter under riot conditions shall pay the entire premium of the political subdivision's health insurance plan for the employee's surviving spouse until remarried, and for each dependent child of the employee until the child reaches the age of majority or until the end of the calendar year in which the child reaches the age of 25 if:

1. At the time of the employee's death, the child is dependent upon the employee for support; and

2. The surviving child continues to be dependent for support, or the surviving child is a full-time or part-time student and is dependent for support.

(g)1. Any employer who employs a full-time firefighter who, on or after January 1, 1995, suffers a catastrophic injury, as defined in s. 440.02, Florida Statutes 2002, in the line of duty shall pay the entire premium of the employer's health insurance plan for the injured employee, the injured employee's spouse, and for each dependent child of the injured employee until the child reaches the age of majority or until the end of the calendar year in which the child reaches the age of 25 if the child continues to be dependent for support, or the child is a full-time or part-time student and is dependent for support. The term "health insurance plan" does not include supplemental

benefits that are not part of the basic group health insurance plan. If the injured employee subsequently dies, the employer shall continue to pay the entire health insurance premium for the surviving spouse until remarried, and for the dependent children, under the conditions outlined in this paragraph. However:

a. Health insurance benefits payable from any other source shall reduce benefits payable under this section.

b. It is unlawful for a person to willfully and knowingly make, or cause to be made, or to assist, conspire with, or urge another to make, or cause to be made, any false, fraudulent, or misleading oral or written statement to obtain health insurance coverage as provided under this paragraph. A person who violates this sub-subparagraph commits a misdemeanor of the first degree, punishable as provided in s. 775.082 or s. 775.083.

c. In addition to any applicable criminal penalty, upon conviction for a violation as described in sub-subparagraph b., a firefighter or other beneficiary who receives or seeks to receive health insurance benefits under this paragraph shall forfeit the right to receive such health insurance benefits, and shall reimburse the employer for all benefits paid due to the fraud or other prohibited activity. For purposes of this sub-subparagraph, the term "conviction" means a determination of guilt that is the result of a plea or trial, regardless of whether adjudication is withheld.

2. In order for the firefighter, spouse, and dependent children to be eligible for such insurance coverage, the injury must have occurred as the result of the firefighter's response to what is reasonably believed to be an emergency involving the





protection of life or property, or an unlawful act perpetrated by another. Except as otherwise provided herein, ~~nothing in~~ this paragraph may not ~~shall~~ be construed to limit health insurance coverage for which the firefighter, spouse, or dependent children may otherwise be eligible, except that a person who qualifies for benefits under this section is ~~shall~~ not ~~be~~ eligible for the health insurance subsidy provided under chapter 121, chapter 175, or chapter 185.

Notwithstanding any provision of this section to the contrary, the death benefits provided in paragraphs (b), (c), and (f) shall also be applicable and paid in cases where a firefighter received bodily injury prior to July 1, 1993, and subsequently died on or after July 1, 1993, as a result of such in-line-of-duty injury.

(h) The Division of the State Fire Marshal within the Department of Financial Services shall adopt rules necessary to implement this section.

~~(i) Any payments made pursuant to paragraph (a), paragraph (b), or paragraph (c) shall consist of the statutory amount adjusted to show price level changes in the Consumer Price Index for All Urban Consumers published by the United States Department of Labor since July 1, 2002. The Division of State Fire Marshal, using the most recent month for which Consumer Price Index data is available, shall, on June 15 of each year, calculate and publish on the division's Internet website the amount resulting from the adjustments to the statutory amounts. The adjusted statutory amounts shall be effective on July 1 of each year.~~

(3) If a firefighter is accidentally killed as specified in paragraph (2)(b) on or after June 22, 1990, but before July 1, 2019, or unlawfully and intentionally killed as specified in paragraph (2)(c), on or after July 1, 1980, but before July 1, 2019, the state must ~~shall~~ waive certain educational expenses that the child or spouse of the deceased firefighter incurs while obtaining a career certificate, an undergraduate education, or a postgraduate education. The amount waived by the state must ~~shall~~ be in an amount equal to the cost of tuition and matriculation and registration fees for a total of 120 credit hours. The child or spouse may attend a state career center, a Florida College System institution, or a state university~~. The child or spouse may attend any or all of the institutions specified in this subsection,~~ on either a full-time or part-time basis. The benefits provided to a child under this subsection shall continue until the child's 25th birthday. The benefits provided to a spouse under this subsection must commence within 5 years after the death occurs, and entitlement thereto shall continue until the 10th anniversary of that death.

(a) Upon failure of any child or spouse who receives a waiver in accordance with ~~benefited by the provisions of~~ this subsection to comply with the ordinary and minimum requirements regarding discipline and scholarship of the institution attended, such ~~both as to discipline and scholarship, the~~ benefits must ~~thereof shall~~ be withdrawn as to the child or spouse and no further moneys expended for the child's or spouse's benefits so long as such failure or delinquency continues.

(b) Only students in good standing in their respective





institutions may ~~shall~~ receive the benefits provided in this subsection ~~thereof~~.

(c) A child or spouse receiving benefits under this subsection must be enrolled according to the customary rules and requirements of the institution attended.

(4)(a) The employer of such firefighter is ~~shall be~~ liable for the payment of the ~~said~~ sums specified in this section and is ~~shall be~~ deemed self-insured, unless it procures and maintains, or has already procured and maintained, insurance to secure such payments. Any such insurance may cover only the risks indicated in this section, in the amounts indicated in this section, or it may cover those risks and additional risks and may be in larger amounts. Any such insurance must ~~shall~~ be placed by such employer only after public bid of such insurance coverage which must ~~coverage shall~~ be awarded to the carrier making the lowest best bid.

(b) Payment of benefits to beneficiaries of state employees, or of the premiums to cover the risk, under ~~the provisions of~~ this section, must ~~shall~~ be paid from existing funds otherwise appropriated for the department.

(5) The State Board of Education shall adopt rules and procedures, and the Board of Governors shall adopt regulations and procedures, as are appropriate and necessary to implement the educational benefits provisions of this section.

Section 3. Section 112.1911, Florida Statutes, is created to read:

112.1911 Emergency medical technicians and paramedics; death benefits.—

(1) As used in this section, the term:

(a) "Emergency medical technician" means a person who is certified by the Department of Health to perform basic life support pursuant to part III of chapter 401, who is employed by an employer, and whose primary duties and responsibilities include on-the-scene emergency medical care.

(b) "Employer" means a state board, commission, department, division, bureau, or agency, or a county, municipality, or other political subdivision of the state.

(c) "Insurance" means insurance procured from a stock company or mutual company, or an association or exchange authorized to do business as an insurer in this state.

(d) "Paramedic" means a person who is certified by the Department of Health to perform basic and advanced life support pursuant to part III of chapter 401, who is employed by an employer, and whose primary duties and responsibilities include on-the-scene emergency medical care.

(2)(a) The sum of $75,000 must be paid as provided in this section when an emergency medical technician or a paramedic, while engaged in the performance of his or her official duties, is accidentally killed or receives an accidental bodily injury that subsequently results in the loss of the individual's life, provided that such killing is not the result of suicide and that such bodily injury is not intentionally self-inflicted.

(b) The sum of $75,000 must be paid as provided in this section if an emergency medical technician or a paramedic is accidentally killed as specified in paragraph (a) and the accidental death occurs as a result of the emergency medical technician's or paramedic's response to what is reasonably believed to be an emergency involving the protection of life.





This sum is in addition to any sum provided under paragraph (a).

(c) If an emergency medical technician or a paramedic, while engaged in the performance of his or her official duties, is unlawfully and intentionally killed or is injured by an unlawful and intentional act of another person and dies as a result of such injury, the sum of $225,000 must be paid as provided in this section.

(d) Such payments, pursuant to paragraphs (a), (b), and (c), whether secured by insurance or not, must be made to the beneficiary designated by such emergency medical technician or paramedic in a written and signed form, which must be delivered to the employer during the emergency medical technician's or paramedic's lifetime. If no such designation is made, then the payments must be made to the emergency medical technician's or paramedic's surviving child or children and to his or her surviving spouse in equal portions, or if there is no surviving child or spouse, must be made to the emergency medical technician's or paramedic's parent or parents. If a beneficiary is not designated and there is no surviving child, spouse, or parent, then the sum must be paid to the emergency medical technician's or paramedic's estate.

(e) Such payments, pursuant to paragraphs (a), (b), and (c), are in addition to any workers' compensation or retirement plan benefits and are exempt from the claims and demands of creditors of such emergency medical technician or paramedic.

(3)(a) The employer of an emergency medical technician or a paramedic is liable for the payment of the benefits specified in this section and is deemed self-insured, unless it procures and maintains, or has already procured and maintained, insurance to

cover such payments. Any such insurance may cover only the risks indicated in this section, in the amounts indicated in this section, or it may cover those risks and additional risks and may be in larger amounts. Any such insurance must be placed by such employer only after public bid of such insurance coverage, which must be awarded to the carrier making the lowest best bid.

(b) Payment of benefits to beneficiaries of state employees, or of the premiums to cover the risk, under this section, must be paid from existing funds otherwise appropriated to the agency that employed the emergency medical technician or paramedic.

Section 4. Section 112.1912, Florida Statutes, is created to read:

112.1912 First responders; death benefits for educational expenses.—

(1) As used in this section, the term "first responder" means:

(a) A law enforcement, correctional, or correctional probation officer as defined in s. 112.19(1) who is killed as provided in s. 112.19(2) on or after July 1, 2019;

(b) A firefighter as defined in s. 112.191(1) who is killed as provided in s. 112.191(2) on or after July 1, 2019; or

(c) An emergency medical technician or a paramedic, as defined in s. 112.1911(1), who is killed as provided in s. 112.1911(2) on or after July 1, 2019.

(2)(a) The state shall waive certain educational expenses that the child or spouse of a deceased first responder incurs while obtaining a career certificate, an undergraduate education, or a postgraduate education. The amount waived by the





state must be in an amount equal to the cost of tuition and matriculation and registration fees for a total of 120 credit hours. The child or the spouse may attend a state career center, a Florida College System institution, or a state university on either a full-time or part-time basis. The benefits provided to a child under this subsection must continue until the child's 25th birthday. The benefits provided to a spouse under this subsection must commence within 5 years after the first responder's death occurs and may continue until the 10th anniversary of that death.

(b) Upon failure of any child or spouse who receives a waiver in accordance with this subsection to comply with the ordinary and minimum requirements regarding discipline and scholarship of the institution attended, such benefits to the child or the spouse must be withdrawn and no further moneys may be expended for the child's or spouse's benefits so long as such failure or delinquency continues.

(c) Only a student in good standing in his or her respective institution may receive the benefits provided in this subsection.

(d) A child or spouse receiving benefits under this subsection must be enrolled according to the customary rules and requirements of the institution attended.

(e) The State Board of Education shall adopt rules and procedures, and the Board of Governors shall adopt regulations and procedures, as are appropriate and necessary to implement this subsection.

Section 5. Subsection (4) of section 250.34, Florida Statutes, is amended to read:

250.34 Injury or death on state active duty.—

(4)(a) The sum of $75,000 must be paid by the state when a ~~Each~~ member of the Florida National Guard, while on state active duty and engaged in the member's official duties, ~~who~~ is accidentally killed or receives accidental bodily injury that results in the loss of the member's life, provided that such killing is not the result of suicide and that such bodily injury is not intentionally self-inflicted.

(b) If a member of the Florida National Guard, while on state active duty and engaged in the performance of the member's official duties, is unlawfully and intentionally killed~~,~~ or ~~who~~ dies as the result of such unlawful and intentional act, the sum of $225,000 must be paid by the state.

(c) Such payments, pursuant to paragraphs (a) and (b), must be made to the beneficiary designated by such member in writing, signed by the member, and delivered to the Florida National Guard during the member's lifetime. If no such designation is made, then the payments must be paid to the member's surviving child or children and to the member's surviving spouse in equal portions, and if there are no surviving children or spouse, then to the member's parent or parents. If a beneficiary is not designated and there is no surviving child, spouse, or parent, then the sum must be paid to the member's estate.

(d) Such payments, pursuant to paragraphs (a) and (b), are exempt from the claims and demands of creditors of such member. ~~injuries incurred, while on state active duty under competent orders qualifies for benefits as a law enforcement officer pursuant to s. 112.19 or any successor statute providing for death benefits for law enforcement officers, and~~





(e) The decedent's survivors or estate are entitled to the death benefits provided in s. 112.19(2)(d) ~~s. 112.19~~. However, this section does not prohibit survivors or the estate of the decedent from presenting a claim bill for approval by the Legislature in addition to the death benefits provided in this section.

(f) If a member of the Florida National Guard is accidentally killed as specified in paragraph (a) or unlawfully and intentionally killed as specified in paragraph (b), the member's surviving child or children and spouse are eligible for the educational benefits as specified in s. 112.1912.

Section 6. Section 295.01, Florida Statutes, is reenacted and amended to read:

295.01 Children of deceased or disabled veterans; spouses of deceased or disabled servicemembers; education.—

(1) It is ~~hereby declared to be~~ the policy of the state to provide educational opportunity at state expense for dependent children either of whose parents entered the Armed Forces and:

(a) Died as a result of service-connected injuries, disease, or disability sustained while on active duty; or

(b) Has been:

1. Determined by the United States Department of Veterans Affairs or its predecessor to have a service-connected 100-percent total and permanent disability rating for compensation;

2. Determined to have a service-connected total and permanent disability rating of 100 percent and is in receipt of disability retirement pay from any branch of the United States Armed Services; or

3. Issued a valid identification card by the Department of

Veterans' Affairs in accordance with s. 295.17,

when the parents of such children have been residents of the state for 1 year immediately preceding the death or the occurrence of such disability, and subject to the rules, restrictions, and limitations set forth in this section.

(2) It is also the declared policy of this state to provide educational opportunity at state expense for spouses of deceased or disabled servicemembers.

(a) The unremarried spouse of a deceased servicemember, as defined in s. 250.01, qualifies for the benefits under this section:

1. If the servicemember and his or her spouse had been residents of the state for 1 year immediately preceding the servicemember's death and the servicemember's death occurred under the circumstances provided in subsection (1); and

2. If the unremarried spouse applies to use the benefit within 5 years after the servicemember's death.

(b) The dependent spouse of a disabled servicemember, as defined in s. 250.01, qualifies for the benefits under this section:

1. If the servicemember and his or her spouse have been married to each other for 1 year; and

2. If the servicemember and his or her spouse have been residents of the state for 1 year immediately preceding the occurrence of the servicemember's disability and the disability meets the criteria set forth in subsection (1); and

3. Only during the duration of the marriage and up to the point of termination of the marriage by dissolution or





annulment.

All rules, restrictions, and limitations set forth in this section shall apply.

(3) Sections 295.03, 295.04, 295.05, and 1009.40 shall apply.

(4) The State Board of Education shall adopt rules for administering this section.

(5) A child or spouse of a servicemember may receive benefits under either this section or s. 295.061.

Section 7. Section 295.061, Florida Statutes, is created to read:

295.061 Active duty servicemembers; death benefits.—

(1) As used in this section, the term:

(a) "Active duty" has the same meaning as provided in s. 250.01.

(b) "United States Armed Forces" means the United States Army, Navy, Air Force, Marine Corps, and Coast Guard.

(2) The sum of $75,000 must be paid by the state if a member of the United States Armed Forces, while on active duty and engaged in the performance of his or her official duties, is killed or receives a bodily injury that results in the loss of the member's life, provided that such killing is not the result of suicide and that such bodily injury is not intentionally self-inflicted.

(3) The sum of $25,000 must be paid by the state if a member of the United States Armed Forces, while on active duty, is killed other than as specified in subsection (2), provided that the killing is not the result of suicide and that such

bodily injury is not intentionally self-inflicted.

(4) Payment of benefits made under subsection (2) or subsection (3) must be paid to the beneficiary designated by such member in writing and delivered to the Department of Military Affairs during the member's lifetime. If no such designation is made, then the payments must be paid to the member's surviving child or children and to his or her surviving spouse in equal portions, or if there is no surviving child or spouse, must be made to the member's parent or parents. If a beneficiary is not designated and there is no surviving child, spouse, or parent, then the sum must be paid to the member's estate.

(5) To qualify for the benefits provided in this section, the deceased military member must have been a resident of this state, or his or her duty post must have been within this state, at the time of death.

(6) Any benefits provided pursuant to this section are in addition to any other benefits provided under the Servicemembers' Group Life Insurance program or any other federal program. Benefits granted pursuant to this section are exempt from the claims and demands of creditors of such member.

(7) Benefits provided under subsection (2) or subsection (3) shall be paid from the General Revenue Fund. Beginning in the 2019-2020 fiscal year and continuing each fiscal year thereafter, a sum sufficient to pay such benefits is appropriated from the General Revenue Fund to the Department of Financial Services for the purposes of paying such benefits.

(8)(a) If an active duty member is killed as specified in subsection (2) or subsection (3), the state must waive certain





educational expenses that the child or the spouse of the deceased member incurs while obtaining a career certificate, an undergraduate education, or a postgraduate education. The amount waived by the state must be in an amount equal to the cost of tuition and matriculation and registration fees for a total of 120 credit hours. The child or the spouse may attend a state career center, a Florida College System institution, or a state university on either a full-time or part-time basis. The benefits provided to a child under this subsection must continue until the child's 25th birthday. The benefits provided to a spouse under this subsection must commence within 5 years after the death occurs and may continue until the 10th anniversary of that death.

(b) Upon failure of any child or spouse who receives a waiver in accordance with this subsection to comply with the ordinary and minimum requirements regarding discipline and scholarship of the institution attended, such benefits to the child or the spouse must be withdrawn and no further moneys may be expended for the child's or spouse's benefits so long as such failure or delinquency continues.

(c) Only a student in good standing in his or her respective institution may receive the benefits provided in this subsection.

(d) A child or spouse who is receiving benefits under this subsection shall be enrolled according to the customary rules and requirements of the institution attended.

(e) A child or spouse of a member may receive benefits under either this subsection or s. 295.01.

(f) The State Board of Education shall adopt rules and

procedures, and the Board of Governors shall adopt regulations and procedures, as are appropriate and necessary to implement this subsection.

Section 8. This act shall take effect July 1, 2019.



**CODING:** Words ~~stricken~~ are deletions; words underlined are additions.

**THE FLORIDA SENATE**

# APPEARANCE RECORD

(Deliver BOTH copies of this form to the Senator or Senate Professional Staff conducting the meeting)

April 16, 2019
*Meeting Date*

7098
*Bill Number (if applicable)*

*Amendment Barcode (if applicable)*

Topic Death Benefits

Name Gary Hester

Job Title Chief - Government Affairs

Address P.O. Box 14083
*Street*

Phone 850-219-3631

Tallahassee FL 32317
*City* *State* *Zip*

Email ghester@fpca.com

Speaking: ☐ For ☐ Against ☐ Information

Waive Speaking: ☑ In Support ☐ Against
*(The Chair will read this information into the record.)*

Representing Florida Police Chiefs Association

Appearing at request of Chair: ☐ Yes ☑ No

Lobbyist registered with Legislature: ☑ Yes ☐ No

*While it is a Senate tradition to encourage public testimony, time may not permit all persons wishing to speak to be heard at this meeting. Those who do speak may be asked to limit their remarks so that as many persons as possible can be heard.*

***This form is part of the public record for this meeting.***

S-001 (10/14/14)

**THE FLORIDA SENATE**

# APPEARANCE RECORD

(Deliver BOTH copies of this form to the Senator or Senate Professional Staff conducting the meeting)

04-16-19
*Meeting Date*

SB 7098
*Bill Number (if applicable)*

Topic DEATH BENEFITS

*Amendment Barcode (if applicable)*

Name CAPTAIN MATT BUTLER

Job Title CAPTAIN LEGISLATIVE AFFAIRS / NARCOTICS

Address 2500 W. COLONIAL DR.
*Street*

Phone 407-254-7000

ORLANDO FL 32805
*City* *State* *Zip*

Email MATT.BUTLER@OCFL.NET

Speaking: ☐ For ☐ Against ☐ Information

Waive Speaking: ☒ In Support ☐ Against
*(The Chair will read this information into the record.)*

Representing ORANGE COUNTY SHERIFF'S OFFICE

Appearing at request of Chair: ☐ Yes ☐ No

Lobbyist registered with Legislature: ☒ Yes ☐ No

*While it is a Senate tradition to encourage public testimony, time may not permit all persons wishing to speak to be heard at this meeting. Those who do speak may be asked to limit their remarks so that as many persons as possible can be heard.*

***This form is part of the public record for this meeting.***

S-001 (10/14/14)

**THE FLORIDA SENATE**

# APPEARANCE RECORD

(Deliver BOTH copies of this form to the Senator or Senate Professional Staff conducting the meeting)

4/16/19
*Meeting Date*

7098
*Bill Number (if applicable)*

Topic Death Benefits

*Amendment Barcode (if applicable)*

Name Rocco Salvatori

Job Title Firefighter

Address 343 W Madison St
*Street*

Phone 850-224-7333

Tallahassee FL 32301
*City* *State* *Zip*

Email RoccoSalvatori@icloud.com

Speaking: ☒ For ☐ Against ☐ Information

Waive Speaking: ☐ In Support ☐ Against
*(The Chair will read this information into the record.)*

Representing Florida Professional Firefighters

Appearing at request of Chair: ☐ Yes ☒ No

Lobbyist registered with Legislature: ☒ Yes ☐ No

*While it is a Senate tradition to encourage public testimony, time may not permit all persons wishing to speak to be heard at this meeting. Those who do speak may be asked to limit their remarks so that as many persons as possible can be heard.*

***This form is part of the public record for this meeting.***

S-001 (10/14/14)

**The Florida Senate**

# BILL ANALYSIS AND FISCAL IMPACT STATEMENT

(This document is based on the provisions contained in the legislation as of the latest date listed below.)

Prepared By: The Professional Staff of the Appropriations Subcommittee on Agriculture, Environment, and General Government

| | |
|---|---|
| BILL: | SB 1570 |
| INTRODUCER: | Senator Hooper |
| SUBJECT: | Information Technology Reorganization |
| DATE: | April 15, 2019 |
| REVISED: | 4/15/19 |

| | ANALYST | STAFF DIRECTOR | REFERENCE | ACTION |
|---|---|---|---|---|
| 1. | Hackett | McVaney | GO | **Favorable** |
| 2. | Davis/Smith | Betta | AEG | **Recommend: Favorable** |
| 3. | | | AP | |

## I. Summary:


SB 1570 makes changes in law relating to state agency information technology. Specifically, the bill:

- Transfers the Agency for State Technology (AST), with all of its existing powers, duties, functions, personnel, records, property, and funds, including the state data center, to the Department of Management Services (DMS) as the newly created Division of State Technology. The bill repeals the statute authorizing the AST.
- Clarifies that the Department of Environmental Protection will review practices related to geospatial data.
- Codifies the Statewide Travel Management System to standardize and maintain records of travel for all state executive and judicial branch agencies.
- Enacts a "cloud-first" policy to require all state agencies to show a preference for cloud-computing systems in their procurements process for new information technology.
- Creates the Cybersecurity Task Force to study cybersecurity procedures, rules, and vulnerabilities and make recommendations thereupon.

The fiscal impact on state expenditures is indeterminate. See Section V.

The bill takes effect July 1, 2019.


## II. Present Situation:

### Agency for State Technology

Chapter 282, F.S., is known as the Enterprise Information Technology Services Management Act.[1]

[1] Section 282.003, F.S.

***General duties***

The Agency for State Technology (AST) was created on July 1, 2014.[2] The executive director of the AST is appointed by the Governor, subject to confirmation by the Senate. The duties and responsibilities of the AST include:[3]

- Developing and publishing information technology (IT) policy for management of the state's IT resources.
- Establishing and publishing IT architecture standards.
- Establishing project management and oversight standards with which state agencies must comply when implementing IT projects.
- Performing project oversight on all state IT projects with total costs of $10 million or more.
- Identifying opportunities for standardization and consolidation of IT services that support common business functions and operations.
- Establishing best practices for procurement of IT products in collaboration with the Department of Management Services (DMS).
- Participating with the DMS in evaluating, conducting and negotiating competitive solicitations for state term contracts for IT commodities, consultant services, or staff augmentation contractual services.
- Collaborating with the DMS in IT resource acquisition planning.
- Developing standards for IT reports and updates.
- Upon request, assisting state agencies in development of IT related legislative budget requests.
- Conducting annual assessments of state agencies to determine compliance with IT standards and guidelines developed by the AST.
- Providing operational management and oversight of the state data center.
- Recommending other IT services that should be designed, delivered, and managed as enterprise IT services.
- Recommending additional consolidations of agency data centers or computing facilities into the state data center.
- In consultation with state agencies, proposing methodology for identifying and collecting current and planned IT expenditure data at the state agency level.
- Performing project oversight on any cabinet agency IT project that has a total project cost of $25 million or more and impacts one or more other agencies.
- Consulting with departments regarding risks and other effects for IT projects implemented by an agency that must be connected to or accommodated by an IT system administered by a cabinet agency.
- Establishing policy for all IT related state contracts, including state term contracts for IT commodities, consultant services, and staff augmentation services in collaboration with the DMS.[4] The IT policy must include:
    - Identification of the IT product and service categories to be included in state term contracts;
    - Requirements to be included in solicitations for state term contracts;

[2] Chapter 2014-221, L.O.F.
[3] Section 282.0051, F.S.
[4] Chapter 2016-138, L.O.F.

- Evaluation criteria for the award of IT-related state term contracts;
- The term of each IT-related state term contract; and
- The maximum number of vendors authorized on each state term contract.

### *Chief Information Officer (CIO)*

The AST is headed by an executive director, established in s. 20.61(1) F.S., who serves as the state's chief information officer and is appointed by the Governor and confirmed by the Senate. Current law requires that the state CIO preferably have executive-level experience in both the public and private sectors in development and implementation of information technology strategic planning; management of enterprise information technology projects, particularly management of large-scale consolidation projects; and development and implementation of fiscal and substantive information technology policy.

### *State Data Center*

The State Data Center is housed within the AST and provides data center services that comply with applicable state and federal laws, regulations, and policies, including all applicable security, privacy, and auditing requirements.[5] The State Data Center must enter into a service-level agreement with each customer entity to provide required type and level of service or services. If a customer fails to execute an agreement within 60 days after commencement of service, the State Data Center may cease service.

State agencies, unless authorized by the Legislature or granted exemption by AST, may not:[6]

- Transfer existing computer services to any data center other than the State Data Center.
- Initiate a new computer service except with the State Data Center.

The State Data Center relies heavily on the use of state-owned equipment installed at the State Data Center facility located in the state's Capital Circle Office Center in Tallahassee for the provision of data center services, often financed through the Department of Financial Services' Consolidated Equipment Financing Program and through lease-purchase arrangements with hardware vendors. This equipment must be replaced periodically, usually around five years.

### *Information Technology Security*

Section 282.318, F.S., establishes the requirements for the security of data and IT. The AST's duties in regards to IT security include:

- Establishing standards and processes for IT security consistent with generally accepted best practices;
- Adopting rules for IT security;
- Developing a statewide IT security strategic plan, updated annually;
- Developing a framework for use by state agencies for IT security responsibilities, such as conducting IT security risk assessments and reporting IT security incidents;
- Providing IT security training for state agency information security managers; and
- Annually reviewing state agency IT security plans.

[5] Section 282.201, F.S.
[6] Section 282.201(5), F.S.

Section 282.318(4)(h), F.S., requires that each state agency head include appropriate IT security requirements in written specifications for the solicitation of IT and IT resources and services that are consistent with the rules and guidelines established by the AST and the DMS.

***Cloud-First Policy***

Cloud computing is the delivery of on-demand computing resources, including data center services, software applications, and data storage, over the Internet on a pay-for-use basis. The definition of cloud computing issued by the National Institute of Standards and Technology (NIST) in Special Publication 800-145 is the most broadly adopted definition of cloud computing.[7] The NIST definition describes the essential characteristics of cloud computing, the types of cloud computing service models, and the types of cloud computing deployment models.

Section 282.0051(6), F.S., provides the duty for the AST to collaborate with the DMS to establish best practices for the procurement of IT products in order to reduce costs, increase productivity, or improve services.

Several states including California, Colorado, Illinois, Michigan, and Texas have adopted a cloud-first policy. Some states have cloud strategies and plans with cloud computing components or are in the process of working to formalize policies and standards for cloud services.[8] The federal government has also implemented a cloud-first policy, first adopted by President Obama in 2011[9] and continued by President Trump in 2017.[10]

State agencies (agencies') are taking advantage of cloud services for their Microsoft office products (Outlook, Excel, Word, etc.) and SharePoint services available on state term contracts.[11] These services are easy to implement and can be supported within their current resources. The more difficult cloud solutions to implement are associated with the agencies' business applications. There are several factors when considering a cloud solution for these applications: current and future IT architecture, age of application and modifications needed for transition, current and future security needs, performance, and IT resources needed for on-going support. Specific Appropriation 2920A of ch. 2015-232, L.O.F., required the AST to contract with a third party consulting firm to conduct a study on the cloud readiness of certain applications hosted at the State Data Center. The vendor completed the Cloud Readiness Study (Study) and provided the findings to the AST.[12] The Study was focused on determining which applications currently housed in the State Data Center were capable of being moved to a third-party, infrastructure-as-a-service (IaaS) cloud solution. A review of 931 applications showed that none of the applications were ready for transition to the cloud.

---

[7] SP 800-145, The NIST Definition of Cloud Computing, (9/2011), National Institute of Standards and Technology.
[8] "State Government Practices for Cloud Implementation", (2015), National Association of State Procurement Officials.
[9] "Federal Cloud Computing Strategy", (2011), Vivek Kundra, Office of the U.S. Chief Information Officer.
[10] Executive Order No. 82 FR 22391, 3 C.F.R. 22391-22397 (2017).
[11] Florida Department of Management Services, Microsoft Enterprise Agreement (State and Local) No. 01E73902, (12/2015), https://www.dms.myflorida.com/content/download/126606/682889/Microsoft_Enterprise_Agreement_(State_and_Local).pdf (last visited Apr. 10, 2019).
[12] Florida Agency for State Technology, *State Data Center Application Cloud Readiness Study*, (Jan. 2016), Grant Thornton. https://static1.squarespace.com/static/58bd820d86e6c0c5a7193736/t/59ea3b79a9db09cb6e415fe2/1508522879652/Cloud+Readiness+Report+01-15-2016.pdf (last visited Apr. 10, 2019).

There are two agencies with projects to move their business application to a cloud solution. The Department of Financial Services is replacing the state's accounting and cash management system with a cloud solution.[13] The project will take nine years and is projected to cost a total of $180 million.[14] The Department of Highway Safety and Motor Vehicles is replacing its drivers and vehicle licensing systems with a cloud solution.[15] The project will take 10 years to complete and is projected to cost $77 million.[16] These projects emphasize the scope, complexity, and cost incurred when addressing the agencies' major applications.

In addition, the Department of Children and Families (DCF) has successfully transitioned their Florida Safe Families Network to a cloud infrastructure solution. The project was completed in Fiscal Year 2017-2018 with transition costs totaling approximately $4 million; the on-going maintenance cost is projected to be $4.9 million,[17] which increased by $2.9 million in the first year.[18] Cloud solutions provide scaleability and improved performance, but these benefits can often come at an additional cost.

**Technology Program in the Department of Management Services**

The Technology Program is organized as the Division of Telecommunications (Division) and provides the state enterprise telecommunications system known as the SUNCOM Network. SUNCOM includes voice, data, radio, wiring and cabling, and conferencing service to state agencies, local governments, educational institutions, libraries, and non-profit organizations.[19] The Division also leads Emergency Support Functions (ESF 2)[20] and E-rate[21] and houses the Bureau of Public Safety, which provides Enhanced 911[22] and radio communications services to the state's public safety entities.[23]

---

[13] Department of Financial Services, Florida Palm. https://www.myfloridacfo.com/floridapalm/ (last visited Apr. 10, 2019).
[14] Department of Financial Services, *Florida Palm Software and System Integrator Contract No.D126*, (July 2018). https://facts.fldfs.com/Search/ContractDetail.aspx?AgencyId=430000&ContractId=D1261 (last visited Apr. 10, 2019).
[15] Department of Highway Safety and Motor Vehicles, available at https://www.flhsmv.gov/motorist-modernization/
[16] Department of Highway Safety and Motor Vehicles, *Motorist Modernization Update* (Feb. 6, 2019) (on file with the Senate Appropriations Subcommittee on Agriculture, Environment, and General Government).
[17] Department of Children and Families, *Proposal to Move the Florida Safe Families Network Application to a Cloud Computing Service*, (Oct. 30, 2015) (on file with the Senate Appropriations Subcommittee on Agriculture, Environment, and General Government).
[18] Department of Children and Families, *Agency Legislative Budget Request Fiscal Year 2018-2019*, D-3A Issue Code 36351C0, available at http://floridafiscalportal.state.fl.us/Document.aspx?ID=17138&DocType=PDF (last visited Apr. 12, 2019).
[19] Section 282.703, F.S.
[20] The DMS, as the lead agency for ESF 2 under the direction of the Division of Emergency Management, is the first point of contract for telecommunications service providers for equipment and services coordination to provide communications support statewide before, during, and after emergencies.
[21] E-Rate is a federal program created to ensure that schools and libraries have affordable access to advance telecommunications services.
[22] Section 365.171, F.S.
[23] Sections 282.709 and 282.7101, F.S.

**Type Two Transfer**

Section 20.06(2), F.S., provides for type two transfers. A type two transfer is the merging into another agency or department of an existing agency or department or a program, activity, or function thereof. A type two transfer preserves the merged entity's statutory powers, duties, rules, and functions, and the merged entity's records, personnel, property, and funds unless specifically severed or abolished. Pursuant to Rule 60L-33.003, F.A.C., if a transfer of an employee is legislatively mandated, the employee retains the status held in the position prior to the time of transfer unless the Legislature directs otherwise. This rule means the employee is transferred to the new entity and retains the employee's status in the originating agency, either probationary status, trainee status, or permanent status.

**Career Service System**

An employee of the state of Florida will generally fall into one of four categories provided by ch. 110, F.S.:

- Career Service System;
- Senior Management System;
- Volunteers; or
- Selected Exempt Service System.

The systems provide the pay schedules, benefits, and certain policies for each class of employee. Section 110.205, F.S., provides that all non-exempt employees belong to the career service system. Section 110.205(2)(e), F.S., exempts the executive director of the AST from the Career Service System. Section 110.205(n), F.S., allows each department head to designate a maximum of 20 policymaking or managerial positions as being exempt from the Career Service System. A department head may additionally designate one position which directly reports to the department head in the Senior Management Service.

**Task Force Requirements under s. 20.03, F.S.**

Section 20.03(8), F.S., defines "task force" to mean an "advisory body created without specific statutory enactment for a time not to exceed one year or created by specific statutory enactment for a time not to exceed three years and appointed to study a specific problem and recommend a solution or policy alternative related to that problem." This provision specifies that the existence of a task force terminates upon the completion of its assignment.

## III. Effect of Proposed Changes:

**Section 1** authorizes a type two transfer of the Agency for State Technology (AST) to the Department of Management Services (DMS) pursuant to s. 20.06(2), F.S. This includes transferring all of the AST's powers, duties, functions, records, offices, personnel, property, issues, contracts, authority, rules, funds, etc. Organizationally, the AST structure is merged with the Technology Program within the DMS (see section 3 below). Pursuant to s. 20.06(2)(c), F.S., all administrative rules of the AST remain in effect after the type two transfer.

**Section 2** provides that all contracts and interagency agreements involving the AST are continued following the transfer.

**Section 3** creates the Division of State Technology (Division) within the DMS, directed by the state chief information officer. This Division is a result of a merger of the existing Technology Program and the AST structure. It sets minimum qualifications for the state chief information officer similar to the current qualifications found in s. 20.61, F.S., but adds a 10-year experience requirement.

**Section 4** continues the transfer of certain duties to the Department of Environmental Protection (DEP), relating to geospatial data, beyond the current expiration date of July 1, 2019. The DEP must review policies, practices, and standards related to all geospatial data managed by state agencies and water management districts. The section allows the DEP to adopt rules to that end.

**Section 5** repeals s. 20.61, F.S., which created the AST.

**Section 6** grants rulemaking authority to the DMS relating to the Statewide Travel Management System. The Statewide Travel Management System is defined as the system developed by the DMS to collect data on, standardize and automate travel management for public officers and employees. The section requires all executive branch state agencies and the judicial branch to report travel using the Statewide Travel Management System. The section also states the travel reports may not reveal confidential or exempt information.

**Section 7** changes the short title for ch. 282, F.S., to the "Information Technology Management Act."

**Section 8** defines the terms "agency assessment," "breach," "cloud computing," "data," and "open data."

**Section 9** amends s. 282.0051, F.S., to shift the current statutory powers, duties, and functions of the AST to the DMS. In addition, the section:

- Removes the duty to review all information technology purchases by state agencies which cost $250,000 or more;
- Requires reports on projected costs for data center services to be sent to the Office of Policy and Budget rather than to each customer entity's agency head; and
- Adds a duty to recommend methods of standardizing data as well as open data technical standards.

**Section 10** amends s. 282.201, F.S., relating to the State Data Center. The section moves the State Data Center from the AST to the DMS, and provides that the DMS will appoint a director for the State Data Center.

In addition, Section 10 requires the State Data Center to enter into service-level agreements with its customers and establish the costs of each service by agency application.

Section 10 also requires the State Data Center to show a preference for cloud-computing solutions in its procurement process, and it must assist customer entities in transitioning from State Data Center use to third-party cloud-computing services.

**Section 11** creates s. 282.206, F.S., to establish a cloud-first policy for state agencies. This policy provides that, in their procurement processes, each state agency shall show a preference for cloud-computing services that does not require, or minimizes, the use of State Data Center infrastructure. It provides that each agency will create procedures for the evaluation of cloud-computing options and a plan with regards to its use of the State Data Center. Each agency must notify the State Data Center by May 31 and November 30 of each year regarding changes in its use of the State Data Center.

**Section 12** amends s. 282.318, F.S., to transfer the current statutory duties relating to information technology security from the AST to the DMS and requires the DMS to designate a state chief information security officer with experience and expertise in security and risk management for communications and IT resources. Agencies must consult with the DMS regarding their IT and cybersecurity needs.

In addition, section 12 requires agency heads ensure that IT security and cybersecurity requirements are included in both the written specifications for the solicitation and service level agreement of IT and IT resources and services meet or exceed the applicable state and federal standards for IT security and cybersecurity. This section also requires that service level agreements identify service provider and state agency responsibilities for privacy and security, protection of government data, personnel background screening, and security deliverables with associated frequencies.

**Section 13** amends s. 17.0315, F.S., to replace the executive director of the AST with the state chief information officer on the task force established to develop a strategic business plan for a successor financial and cash management system.

**Section 14** amends s. 20.055, F.S., to remove the reference to the AST in the definition of "state agency."

**Section 15** amends s. 97.0525, F.S., to replace the AST with the DMS in a reference to their risk assessment methodology for identifying security risks.

**Section 16** amends s. 110.205, F.S., to exempt the chief information officer from the state career service. Division heads are separately exempt under s. 110.205(j), F.S. In moving from an agency to a division head position, the AST structure will no longer be provided 20 designated exempt positions. Those positions will fall under the DMS's umbrella and no longer be exempt unless designated by the head of the DMS.

**Section 17** amends s. 215.322, F.S., to provide the state chief information officer, rather than the AST, must review requests to use electronic collection methods and consult with the chief financial officer on uniform security safeguards for cardholder data.

**Section 18** amends s. 215.96, F.S., to replace the executive director of the AST with the state chief information officer on the coordinating council under the Florida Financial Management Information System Act.

**Section 19** amends s. 287.057, F.S., to replace the AST with the chief information officer as the consulting entity for the DMS maintaining a program for online procurement of commodities and contractual services.

**Section 20** amends s. 282.00515, F.S., replaces the AST with the DMS as the body with whom several departments may contract for various technological services under s. 282.0051, F.S.

**Section 21** amends s. 287.0591, F.S., to replace the executive director of the AST with the state chief information officer as the person who may certify that long term contracts are beneficial to the state. It also states that the Division, rather than the AST, may participate in the DMS's competitive solicitations for information technology commodities, consultant services, or staff augmentation services.

**Section 22** amends s. 365.171, F.S., to replace the Technology Program with the Division in the definition for "office" as used in s. 365.171, F.S., emergency communications number "E911."

**Section 23** amends s. 365.172, F.S., to replace the Technology Program with the Division in the definition for "office" as used in ss. 365.171, 365.172, 365.173, and 365.174, F.S., emergency communications number E911 state plan.

**Section 24** amends s. 365.173, F.S., to replace the Technology Program with the Division as the location of the Emergency Communications Number E911 System Fund created to hold revenue from fees and subscriptions in the E911 system.

**Sections 25 and 26** amend ss. 445.011 and 445.045, F.S., to replace the executive director of the AST with the state chief information officer as the person with whom CareerSource Florida, Inc., shall coordinate.

**Section 27** amends s. 668.50, F.S., to replace the AST with the DMS as the body who may specify various regulations and procedures regarding electronic records under the Uniform Electronic Transaction Act.

**Section 28** amends s. 943.0415, F.S., to replace the AST with the DMS as the body with whom the Cybercrime Office of the Florida Department of Law Enforcement (FDLE) is to consult.

**Section 29** creates the Florida Cybersecurity Task Force (task force) and requires administrative support by the DMS. The task force is to:

- Recommend methods to secure the State's network systems and data;
- Identify and recommend remedy for high-risk cybersecurity issues;
- Recommend a process to regularly assess cybersecurity infrastructure;
- Identify gaps in the state's cybersecurity infrastructure;
- Recommend improvements to the cybersecurity of emergency management and disaster response systems;

- Recommend cybersecurity improvements for the state data center; and
- Recommend improvements relating to the state's operational plans for the response to a cybersecurity attack.

The task force is to be chaired by the Lieutenant Governor or his or her designee, and composed of at least nine additional members, to include:

- A representative of the Computer Crime Center of the FDLE;
- A representative of the Fusion Center of the FDLE;
- The state chief information officer;
- The state chief information security officer;
- A representative of the Division of Emergency Management;
- A representative of the Office of the Chief Inspector General;
- An individual appointed by the President of the Senate;
- An individual appointed by the Speaker of the House of Representatives; and
- Members of the private sector appointed by the Governor.

The task force is required to convene by October 1, 2019, meet at least quarterly, and submit a final report of its findings and recommendations to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives by November 1, 2020. The bill abolishes the task force on January 1, 2021.

**Section 30** provides that the bill shall take effect July 1, 2019.

## IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

Not applicable. The bill does not require counties and municipalities to spend funds, reduce counties' or municipalities' ability to raise revenue, or reduce the percentage of a state tax shares with counties and municipalities.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

D. State Tax or Fee Increases:

None.

E. Other Constitutional Issues:

None identified.

## V. Fiscal Impact Statement:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

Vendors offering a cloud solution may be more likely to be awarded information technology (IT) procurements under the "cloud-first" policy established in this bill.

C. Government Sector Impact:

The fiscal impact of the bill on state expenditures is indeterminate. The "cloud-first" policy may result in increased costs to the state agencies. It appears that state agencies must show some preference to a private vendor providing a cloud-computing solution over a similar cloud-computing solution provided by the State Data Center, without regard to the costs of the procured solution.

The State Data Center may see a decrease in utilization as agencies migrate to the cloud, thus reducing the State Data Center's assessment for services in the fiscal year proceeding the drop in utilization.

The bill provides for the transfer of 203 positions, $44,002 from the General Revenue Fund, and $64.3 million in trust fund authority from the Agency for State Technology to the Department of Management Services.

## VI. Technical Deficiencies:

**Section 6** amends s. 112.061, F.S., to codify the Statewide Travel Management System. Line 197-198 states the purpose of the system is to "collect and store information relating to public officer and employee travel information." Public officers and employees, for purposes of chapter 112, F.S., include local government officers and employees as well as state officers and employees. Lines 203-204 require state executive branch agencies and the judicial branch to report travel information on the system. Lines 209-213 require state executive branch agencies and the judicial branch to use the system for travel authorization and reimbursement. If the use of the Statewide Travel Management System is intended to be limited to state public officers and employees, the Legislature may want to consider modifying lines 197-198 to read "collect and store information relating to state executive branch and judicial branch travel information."

**Section 16** amends s. 110.205(e), F.S., to exempt the chief information officer from the state career service. Because the chief information officer is the director of the Division of State Technology, that position is exempted pursuant to s. 110.205(j), F.S. Section 16 could simply be repealed so that no confusion occurs.

**Section 29** creates the Florida Cybersecurity Task Force (task force) within the Department of Management Services (DMS). Lines 1460-1461 of the bill state that the task force will operate in a manner consistent with s. 20.052, F.S. Section 20.052, F.S., and requires the private citizen

members of an advisory body that is adjunct to an executive branch agency to be appointed by the Governor, the head of the department, the executive director of the department, or a Cabinet officer. If the task force must operate consistent with this requirement, the appointments by the President of the Senate and the Speaker of the House of Representatives may not be private citizens (most likely must be members of the Legislature).

The task force is composed of a representative of the Florida Department of Law Enforcement (FDLE) Computer Crime Center, a representative of the FDLE Fusion Center, the state chief information officer and the state chief information security officer, and others. These four state employees may have an on-going working relationship required to effectively accomplish their various job duties. However, as a member of the same advisory body, subject to public meetings requirements, these four state employees may not be able to communicate for their normal job duties if their discussions include topics addressed by the task force.

## VII. Related Issues:

**Section 11** establishes a "cloud-first" policy for state agencies. The state agencies are directed to "show a preference for cloud-computing solutions that either minimize or do not require the use of state data center infrastructure when cloud-computing solutions meet the needs of the agency, reduce costs, and meet or exceed the applicable state and federal laws, regulations, and standards for information technology (IT) security." From the client agency's point of view, the state data center may be providing "cloud-computing." Stated another way, this cloud-first policy appears to direct state agencies to show a preference for private vendors providing cloud-computing over the state data center providing cloud-computing with new infrastructure. This may result in the client agency paying higher costs for IT solutions to the extent that the state data center solution is less expensive than the private vendor solution.

**Section 29** creates the Florida Cybersecurity Task Force to review various IT security issues. Pursuant to s 20.052(5)(c), F.S., a meeting of an advisory body is a public meeting under s. 286.011, F.S., unless otherwise authorized. The public nature of the meetings may hinder open communication among the task force members. Section 286.0113, F.S., provides that a portion of a meeting that would reveal a security or firesafety system plan or portion thereof made confidential by s. 119.071(3)(a), F.S., is exempt from the public meetings requirements of s. 286.011 and s. 24(b), Art. I of the State Constitution. However, most of the IT security information is made confidential and exempt under the provisions of s. 282.318, F.S. Thus, the exemption from public meetings requirements does not appear to apply.

Likewise, there is a concern regarding the use of confidential and exempt information by the task force, particularly if persons not employed by the state are appointed to the task force. Information relating to IT security is typically confidential and exempt. Such information may be available to the Auditor General, the Cybercrime Office, the Chief Inspector General, and now, under the bill, the Division of State Technology of the Department of Management Services (DMS). It is unclear whether state agencies will be permitted to share confidential and exempt information with the task force. Note that the task force is adjunct to the DMS and is not related to the Division of State Technology. The Florida Department of Law Enforcement (FDLE) has recommended incorporating language into the task force providing that any confidential or

exempt information the task force obtains remains confidential or exempt in the hands of the task force.

## VIII. Statutes Affected:

This bill substantially amends the following sections of the Florida Statutes: 20.22, 20.255, 112.061, 282.003, 282.0041, 282.0051, 282.201, 282.318, 17.0315, 20.055, 97.0525, 110.205, 215.322, 215.96, 287.057, 282.00515, 287.0591, 365.171, 365.172, 365.173, 445.011, 445.045, 668.50, and 943.0415.

This bill creates section 282.206 of the Florida Statutes.

This bill repeals section 20.61 of the Florida Statutes.

## IX. Additional Information:

### A. Committee Substitute – Statement of Changes:
(Summarizing differences between the Committee Substitute and the prior version of the bill.)

None.

### B. Amendments:

None.

**By** Senator Hooper

16-01145-19 20191570__

A bill to be entitled

An act relating to information technology reorganization; transferring all powers, duties, functions, records, offices, personnel, associated administrative support positions, property, pending issues and existing contracts, administrative authority, certain administrative rules, trust funds, and unexpended balances of appropriations, allocations, and other funds of the Agency for State Technology to the Department of Management Services by a type two transfer; providing for the continuation of certain contracts and interagency agreements; amending s. 20.22, F.S.; establishing the Division of State Technology within the Department of Management Services to supersede the Technology Program; establishing the position of state chief information officer and providing qualifications thereof; amending s. 20.255, F.S.; removing the expiration for provisions designating the Department of Environmental Protection as the lead agency for geospatial data; authorizing the department to adopt rules for specified purposes; repealing s. 20.61, F.S., relating to the Agency for State Technology; amending s. 112.061, F.S.; authorizing the Department of Management Services to adopt rules for certain purposes; defining the term "statewide travel management system"; specifying reporting requirements for executive branch agencies and the judicial branch through the statewide travel management system;



**CODING:** Words ~~stricken~~ are deletions; words underlined are additions.



16-01145-19 20191570__

specifying that travel reports on the system may not reveal confidential or exempt information; amending s. 282.003, F.S.; revising a short title; reordering and amending s. 282.0041, F.S.; revising and providing definitions; amending s. 282.0051, F.S.; transferring powers, duties, and functions of the Agency for State Technology to the Department of Management Services and revising such powers, duties, and functions; removing certain project oversight requirements; requiring agency projected costs for data center services to be provided to the Governor and the Legislature on an annual basis; requiring the department to provide certain recommendations; amending s. 282.201, F.S.; transferring the state data center from the Agency for State Technology to the Department of Management Services; requiring the department to appoint a director of the state data center; deleting legislative intent; revising duties of the state data center; requiring the state data center to show preference for cloud-computing solutions in its procurement process; revising the use of the state data center and certain consolidation requirements; removing obsolete language; revising agency limitations; creating s. 282.206, F.S.; providing legislative intent regarding the use of cloud computing; requiring each state agency to adopt formal procedures for cloud-computing options; requiring a state agency to develop, and update annually, a strategic plan for submission to the



**CODING:** Words ~~stricken~~ are deletions; words underlined are additions.

Governor and the Legislature; specifying requirements for the strategic plan; requiring a state agency customer entity to notify the state data center biannually of changes in anticipated use of state data center services; specifying requirements and limitations as to cloud-computing services for the Department of Law Enforcement; amending s. 282.318, F.S.; requiring the Department of Management Services to appoint a state chief information security officer; revising and specifying requirements for service-level agreements for information technology and information technology resources and services; conforming provisions to changes made by the act; amending ss. 17.0315, 20.055, 97.0525, 110.205, 215.322, 215.96, 287.057, 282.00515, 287.0591, 365.171, 365.172, 365.173, 445.011, 445.045, 668.50, and 943.0415, F.S.; conforming provisions and a cross-reference to changes made by the act; creating the Florida Cybersecurity Task Force; providing for the membership, meeting requirements, and duties of the task force; providing for administrative and staff support; requiring executive branch departments and agencies to cooperate with information requests made by the task force; providing reporting requirements; providing for expiration of the task force; providing an effective date.

Be It Enacted by the Legislature of the State of Florida:





Section 1. All powers; duties; functions; records; offices; personnel; associated administrative support positions; property; pending issues and existing contracts; administrative authority; administrative rules in chapter 74, Florida Administrative Code, in effect as of July 1, 2019; trust funds; and unexpended balances of appropriations, allocations, and other funds of the Agency for State Technology are transferred by a type two transfer pursuant to s. 20.06(2), Florida Statutes, to the Department of Management Services.

Section 2. Any contract or interagency agreement existing before July 1, 2019, between the Agency for State Technology, or any entity or agent of the agency, and any other agency, entity, or person shall continue as a contract or agreement on the successor department or entity responsible for the program, activity, or function relative to the contract or agreement.

Section 3. Paragraph (b) of subsection (2) and subsection (4) of section 20.22, Florida Statutes, are amended to read:

20.22 Department of Management Services.—There is created a Department of Management Services.

(2) The following divisions and programs within the Department of Management Services are established:

(b) Division of State Technology, the director of which is appointed by the secretary of the department and shall serve as the state chief information officer. The state chief information officer must be a proven, effective administrator who must have at least 10 years of executive-level experience in the public or private sector, preferably with experience in the development of information technology strategic planning and the development and implementation of fiscal and substantive information

technology policy and standards ~~Technology Program~~.

~~(4) The Department of Management Services shall provide the Agency for State Technology with financial management oversight. The agency shall provide the department all documents and necessary information, as requested, to meet the requirements of this section. The department's financial management oversight includes:~~

~~(a) Developing and implementing cost-recovery mechanisms for the administrative and data center costs of services through agency assessments of applicable customer entities. Such cost-recovery mechanisms must comply with applicable state and federal regulations concerning the distribution and use of funds and must ensure that, for each fiscal year, no service or customer entity subsidizes another service or customer entity.~~

~~(b) Implementing an annual reconciliation process to ensure that each customer entity is paying for the full direct and indirect cost of each service as determined by the customer entity's use of each service.~~

~~(c) Providing rebates that may be credited against future billings to customer entities when revenues exceed costs.~~

~~(d) Requiring each customer entity to transfer sufficient funds into the appropriate data processing appropriation category before implementing a customer entity's request for a change in the type or level of service provided, if such change results in a net increase to the customer entity's costs for that fiscal year.~~

~~(e) By October 1, 2018, providing to each customer entity's agency head the estimated agency assessment cost by the Agency for State Technology for the following fiscal year. The agency~~



**CODING:** Words ~~stricken~~ are deletions; words underlined are additions.



~~assessment cost of each customer entity includes administrative and data center services costs of the agency.~~

~~(f) Preparing the legislative budget request for the Agency for State Technology based on the issues requested and approved by the executive director of the Agency for State Technology. Upon the approval of the agency's executive director, the Department of Management Services shall transmit the agency's legislative budget request to the Governor and the Legislature pursuant to s. 216.023.~~

~~(g) Providing a plan for consideration by the Legislative Budget Commission if the Agency for State Technology increases the cost of a service for a reason other than a customer entity's request made under paragraph (d). Such a plan is required only if the service cost increase results in a net increase to a customer entity.~~

~~(h) Providing a timely invoicing methodology to recover the cost of services provided to the customer entity pursuant to s. 215.422.~~

~~(i) Providing an annual reconciliation process of prior year expenditures completed on a timely basis and overall budget management pursuant to chapter 216.~~

~~(j) This subsection expires July 1, 2019.~~

Section 4. Subsection (9) of section 20.255, Florida Statutes, is amended to read:

20.255 Department of Environmental Protection.—There is created a Department of Environmental Protection.

(9) The department shall act as the lead agency of the executive branch for the development and review of policies, practices, and standards related to geospatial data managed by



**CODING:** Words ~~stricken~~ are deletions; words underlined are additions.

state agencies and water management districts. The department shall coordinate and promote geospatial data sharing throughout ~~the~~ state government and serve as the primary point of contact for statewide geographic information systems projects, grants, and resources. The department may adopt rules pursuant to ss. 120.536(1) and 120.54 to implement this subsection ~~This subsection expires July 1, 2019~~.

Section 5. Section 20.61, Florida Statutes, is repealed.

Section 6. Paragraph (c) is added to subsection (9) of section 112.061, Florida Statutes, and subsection (16) is added to that section, to read:

112.061 Per diem and travel expenses of public officers, employees, and authorized persons; statewide travel management system.—

(9) RULES.—

(c) The Department of Management Services may adopt rules to administer the provisions of this section which relate to the statewide travel management system.

(16) STATEWIDE TRAVEL MANAGEMENT SYSTEM.—

(a) For purposes of this subsection, "statewide travel management system" means the system developed by the Department of Management Services to:

1. Collect and store information relating to public officer or employee travel information;

2. Standardize and automate agency travel management;

3. Allow for travel planning and approval, expense reporting, and reimbursement; and

4. Allow travel information queries.

(b) Each executive branch state government agency and the





judicial branch must report on the statewide travel management system all public officer and employee travel information, including, but not limited to, name and position title; purpose of travel; dates and location of travel; mode of travel; confirmation from the head of the agency or designee authorization, if required; and total travel cost. Each executive branch state government agency and the judicial branch must use the statewide travel management system for purposes of travel authorization and reimbursement.

(c) Travel reports made available on the statewide travel management system may not reveal information made confidential or exempt by law.

Section 7. Section 282.003, Florida Statutes, is amended to read:

282.003 Short title.—This part may be cited as the "~~Enterprise~~ Information Technology ~~Services~~ Management Act."

Section 8. Effective July 1, 2019, and upon the expiration of the amendment to that section made by chapter 2018-10, Laws of Florida, section 282.0041, Florida Statutes, is reordered and amended to read:

282.0041 Definitions.—As used in this chapter, the term:

(1) "Agency assessment" means the amount each customer entity must pay annually for services from the Department of Management Services and includes administrative and data center services costs.

(2) ~~(1)~~ "Agency data center" means agency space containing 10 or more physical or logical servers.

(3) ~~(2)~~ "Breach" has the same meaning as provided in s. 501.171 ~~means a confirmed event that compromises the~~

~~confidentiality, integrity, or availability of information or data~~.

(4) ~~(3)~~ "Business continuity plan" means a collection of procedures and information designed to keep an agency's critical operations running during a period of displacement or interruption of normal operations.

(5) "Cloud computing" has the same meaning as provided in Special Publication 800-145 issued by the National Institute of Standards and Technology.

(6) ~~(4)~~ "Computing facility" or "agency computing facility" means agency space containing fewer than a total of 10 physical or logical servers, but excluding single, logical-server installations that exclusively perform a utility function such as file and print servers.

(7) ~~(5)~~ "Customer entity" means an entity that obtains services from the Department of Management Services ~~state data center~~.

(8) "Data" means a subset of structured information in a format that allows such information to be electronically retrieved and transmitted.

(9) ~~(6)~~ "Department" means the Department of Management Services.

(10) ~~(7)~~ "Disaster recovery" means the process, policies, procedures, and infrastructure related to preparing for and implementing recovery or continuation of an agency's vital technology infrastructure after a natural or human-induced disaster.

(11) ~~(8)~~ "Enterprise information technology service" means an information technology service that is used in all agencies





or a subset of agencies and is established in law to be designed, delivered, and managed at the enterprise level.

(12) ~~(9)~~ "Event" means an observable occurrence in a system or network.

(13) ~~(10)~~ "Incident" means a violation or imminent threat of violation, whether such violation is accidental or deliberate, of information technology resources, security ~~policies~~, ~~acceptable use~~ policies, or ~~standard security~~ practices. An imminent threat of violation refers to a situation in which the state agency has a factual basis for believing that a specific incident is about to occur.

(14) ~~(11)~~ "Information technology" means equipment, hardware, software, firmware, programs, systems, networks, infrastructure, media, and related material used to automatically, electronically, and wirelessly collect, receive, access, transmit, display, store, record, retrieve, analyze, evaluate, process, classify, manipulate, manage, assimilate, control, communicate, exchange, convert, converge, interface, switch, or disseminate information of any kind or form.

(15) ~~(12)~~ "Information technology policy" means a definite course or method of action selected from among one or more alternatives that guide and determine present and future decisions.

(16) ~~(13)~~ "Information technology resources" has the same meaning as provided in s. 119.011.

(17) ~~(14)~~ "Information technology security" means the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of data, information, and

information technology resources.

(18) "Open data" means data collected or created by a state agency and structured in a way that enables the data to be fully discoverable and usable by the public. The term does not include data that are restricted from public distribution based on federal or state privacy, confidentiality, and security laws and regulations or data for which a state agency is statutorily authorized to assess a fee for its distribution.

(19) ~~(15)~~ "Performance metrics" means the measures of an organization's activities and performance.

(20) ~~(16)~~ "Project" means an endeavor that has a defined start and end point; is undertaken to create or modify a unique product, service, or result; and has specific objectives that, when attained, signify completion.

(21) ~~(17)~~ "Project oversight" means an independent review and analysis of an information technology project that provides information on the project's scope, completion timeframes, and budget and that identifies and quantifies issues or risks affecting the successful and timely completion of the project.

(22) ~~(18)~~ "Risk assessment" means the process of identifying security risks, determining their magnitude, and identifying areas needing safeguards.

(23) ~~(19)~~ "Service level" means the key performance indicators (KPI) of an organization or service which must be regularly performed, monitored, and achieved.

(24) ~~(20)~~ "Service-level agreement" means a written contract between the Department of Management Services ~~state data center~~ and a customer entity which specifies the scope of services provided, service level, the duration of the agreement, the





responsible parties, and service costs. A service-level agreement is not a rule pursuant to chapter 120.

(25) ~~(21)~~ "Stakeholder" means a person, group, organization, or state agency involved in or affected by a course of action.

(26) ~~(22)~~ "Standards" means required practices, controls, components, or configurations established by an authority.

(27) ~~(23)~~ "State agency" means any official, officer, commission, board, authority, council, committee, or department of the executive branch of state government; the Justice Administrative Commission; and the Public Service Commission. The term does not include university boards of trustees or state universities. As used in part I of this chapter, except as otherwise specifically provided, the term does not include the Department of Legal Affairs, the Department of Agriculture and Consumer Services, or the Department of Financial Services.

(28) ~~(24)~~ "SUNCOM Network" means the state enterprise telecommunications system that provides all methods of electronic or optical telecommunications beyond a single building or contiguous building complex and used by entities authorized as network users under this part.

(29) ~~(25)~~ "Telecommunications" means the science and technology of communication at a distance, including electronic systems used in the transmission or reception of information.

(30) ~~(26)~~ "Threat" means any circumstance or event that has the potential to adversely impact a state agency's operations or assets through an information system via unauthorized access, destruction, disclosure, or modification of information or denial of service.

(31) ~~(27)~~ "Variance" means a calculated value that

illustrates how far positive or negative a projection has deviated when measured against documented estimates within a project plan.

Section 9. Effective July 1, 2019, and upon the expiration of the amendment to that section made by chapter 2018-10, Laws of Florida, section 282.0051, Florida Statutes, is amended to read:

282.0051 Department of Management Services ~~Agency for State Technology~~; powers, duties, and functions.—The department ~~Agency for State Technology~~ shall have the following powers, duties, and functions:

(1) Develop and publish information technology policy for the management of the state's information technology resources.

(2) Establish and publish information technology architecture standards to provide for the most efficient use of the state's information technology resources and to ensure compatibility and alignment with the needs of state agencies. The department ~~agency~~ shall assist state agencies in complying with the standards.

(3) ~~By June 30, 2015,~~ Establish project management and oversight standards with which state agencies must comply when implementing information technology projects. The department ~~agency~~ shall provide training opportunities to state agencies to assist in the adoption of the project management and oversight standards. To support data-driven decisionmaking, the standards must include, but are not limited to:

(a) Performance measurements and metrics that objectively reflect the status of an information technology project based on a defined and documented project scope, cost, and schedule.





(b) Methodologies for calculating acceptable variances in the projected versus actual scope, schedule, or cost of an information technology project.

(c) Reporting requirements, including requirements designed to alert all defined stakeholders that an information technology project has exceeded acceptable variances defined and documented in a project plan.

(d) Content, format, and frequency of project updates.

(4) ~~Beginning January 1, 2015,~~ Perform project oversight on all state agency information technology projects that have total project costs of $10 million or more and that are funded in the General Appropriations Act or any other law. The department ~~agency~~ shall report at least quarterly to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives on any information technology project that the department ~~agency~~ identifies as high-risk due to the project exceeding acceptable variance ranges defined and documented in a project plan. The report must include a risk assessment, including fiscal risks, associated with proceeding to the next stage of the project, and a recommendation for corrective actions required, including suspension or termination of the project.

(5) ~~By April 1, 2016, and biennially thereafter,~~ Identify opportunities for standardization and consolidation of information technology services that support business functions and operations, including administrative functions such as purchasing, accounting and reporting, cash management, and personnel, and that are common across state agencies. The department ~~agency~~ shall biennially on April 1 provide

recommendations for standardization and consolidation to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives. ~~The agency is not precluded from providing recommendations before April 1, 2016.~~

(6) ~~In collaboration with the Department of Management Services,~~ Establish best practices for the procurement of information technology products and cloud-computing services in order to reduce costs, increase the quality of data center services ~~productivity~~, or improve government services. ~~Such practices must include a provision requiring the agency to review all information technology purchases made by state agencies that have a total cost of $250,000 or more, unless a purchase is specifically mandated by the Legislature, for compliance with the standards established pursuant to this section.~~

(7) ~~(a) Participate with the Department of Management Services in evaluating, conducting, and negotiating competitive solicitations for state term contracts for information technology commodities, consultant services, or staff augmentation contractual services pursuant to s. 287.0591.~~

~~(b) Collaborate with the Department of Management Services in information technology resource acquisition planning.~~

~~(8)~~ Develop standards for information technology reports and updates, including, but not limited to, operational work plans, project spend plans, and project status reports, for use by state agencies.

(8) ~~(9)~~ Upon request, assist state agencies in the development of information technology-related legislative budget



**CODING:** Words ~~stricken~~ are deletions; words underlined are additions.



requests.

(9) ~~(10) Beginning July 1, 2016, and annually thereafter,~~ Conduct annual assessments of state agencies to determine compliance with all information technology standards and guidelines developed and published by the department ~~agency, and beginning December 1, 2016, and annually thereafter,~~ and provide results of the assessments to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives.

(10) ~~(11)~~ Provide operational management and oversight of the state data center established pursuant to s. 282.201, which includes:

(a) Implementing industry standards and best practices for the state data center's facilities, operations, maintenance, planning, and management processes.

(b) Developing and implementing cost-recovery mechanisms that recover the full direct and indirect cost of services through charges to applicable customer entities. Such cost-recovery mechanisms must comply with applicable state and federal regulations concerning distribution and use of funds and must ensure that, for any fiscal year, no service or customer entity subsidizes another service or customer entity.

(c) Developing and implementing appropriate operating guidelines and procedures necessary for the state data center to perform its duties pursuant to s. 282.201. The guidelines and procedures must comply with applicable state and federal laws, regulations, and policies and conform to generally accepted governmental accounting and auditing standards. The guidelines and procedures must include, but need not be limited to:



**CODING:** Words ~~stricken~~ are deletions; words underlined are additions.

1. Implementing a consolidated administrative support structure responsible for providing financial management, procurement, transactions involving real or personal property, human resources, and operational support.

2. Implementing an annual reconciliation process to ensure that each customer entity is paying for the full direct and indirect cost of each service as determined by the customer entity's use of each service.

3. Providing rebates that may be credited against future billings to customer entities when revenues exceed costs.

4. Requiring customer entities to validate that sufficient funds exist in the appropriate data processing appropriation category or will be transferred into the appropriate data processing appropriation category before implementation of a customer entity's request for a change in the type or level of service provided, if such change results in a net increase to the customer entity's cost for that fiscal year.

5. By November 15 ~~September 1~~ of each year, providing to the Office of Policy and Budget in the Executive Office of the Governor and to the chairs of the legislative appropriations committees ~~each customer entity's agency head~~ the projected costs of providing data center services for the following fiscal year.

6. Providing a plan for consideration by the Legislative Budget Commission if the cost of a service is increased for a reason other than a customer entity's request made pursuant to subparagraph 4. Such a plan is required only if the service cost increase results in a net increase to a customer entity for that fiscal year.





7. Standardizing and consolidating procurement and contracting practices.

(d) In collaboration with the Department of Law Enforcement, developing and implementing a process for detecting, reporting, and responding to information technology security incidents, breaches, and threats.

(e) Adopting rules relating to the operation of the state data center, including, but not limited to, budgeting and accounting procedures, cost-recovery methodologies, and operating procedures.

(f) ~~Beginning May 1, 2016, and annually thereafter,~~ Conducting an annual ~~a~~ market analysis to determine whether the state's approach to the provision of data center services is the most effective and cost-efficient ~~efficient~~ manner by which its customer entities can acquire such services, based on federal, state, and local government trends; best practices in service provision; and the acquisition of new and emerging technologies. The results of the market analysis shall assist the state data center in making adjustments to its data center service offerings.

(11)~~(12)~~ Recommend other information technology services that should be designed, delivered, and managed as enterprise information technology services. Recommendations must include the identification of existing information technology resources associated with the services, if existing services must be transferred as a result of being delivered and managed as enterprise information technology services.

~~(13) Recommend additional consolidations of agency computing facilities or data centers into the state data center~~

~~established pursuant to s. 282.201. Such recommendations shall include a proposed timeline for consolidation.~~

(12)~~(14)~~ In consultation with state agencies, propose a methodology and approach for identifying and collecting both current and planned information technology expenditure data at the state agency level.

(13)(a) ~~(15)(a) Beginning January 1, 2015, and~~ Notwithstanding any other law, provide project oversight on any information technology project of the Department of Financial Services, the Department of Legal Affairs, and the Department of Agriculture and Consumer Services which ~~that~~ has a total project cost of $25 million or more and which ~~that~~ impacts one or more other agencies. Such information technology projects must also comply with the applicable information technology architecture, project management and oversight, and reporting standards established by the department ~~agency~~.

(b) When performing the project oversight function specified in paragraph (a), report at least quarterly to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives on any information technology project that the department ~~agency~~ identifies as high-risk due to the project exceeding acceptable variance ranges defined and documented in the project plan. The report shall include a risk assessment, including fiscal risks, associated with proceeding to the next stage of the project and a recommendation for corrective actions required, including suspension or termination of the project.

(14)~~(16)~~ If an information technology project implemented by a state agency must be connected to or otherwise accommodated





by an information technology system administered by the Department of Financial Services, the Department of Legal Affairs, or the Department of Agriculture and Consumer Services, consult with these departments regarding the risks and other effects of such projects on their information technology systems and work cooperatively with these departments regarding the connections, interfaces, timing, or accommodations required to implement such projects.

(15)~~(17)~~ If adherence to standards or policies adopted by or established pursuant to this section causes conflict with federal regulations or requirements imposed on a state agency and results in adverse action against the state agency or federal funding, work with the state agency to provide alternative standards, policies, or requirements that do not conflict with the federal regulation or requirement. ~~Beginning July 1, 2015,~~ The department ~~agency~~ shall annually report such alternative standards to the Governor, the President of the Senate, and the Speaker of the House of Representatives.

(16)~~(18) In collaboration with the Department of Management Services:~~

(a) Establish an information technology policy for all information technology-related state contracts, including state term contracts for information technology commodities, consultant services, and staff augmentation services. The information technology policy must include:

1. Identification of the information technology product and service categories to be included in state term contracts.

2. Requirements to be included in solicitations for state term contracts.

3. Evaluation criteria for the award of information technology-related state term contracts.

4. The term of each information technology-related state term contract.

5. The maximum number of vendors authorized on each state term contract.

(b) Evaluate vendor responses for information technology-related state term contract solicitations and invitations to negotiate.

(c) Answer vendor questions on information technology-related state term contract solicitations.

(d) Ensure that the information technology policy established pursuant to paragraph (a) is included in all solicitations and contracts that ~~which~~ are administratively executed by the department.

(17) Recommend potential methods for standardizing data across state agencies which will promote interoperability and reduce the collection of duplicative data.

(18) Recommend open data technical standards and terminologies for use by state agencies.

(19) Adopt rules to administer this section.

Section 10. Effective July 1, 2019, and upon the expiration of the amendment to that section made by chapter 2018-10, Laws of Florida, section 282.201, Florida Statutes, is amended to read:

282.201 State data center.—The state data center is established within the department ~~Agency for State Technology and shall provide data center services that are hosted on premises or externally through a third-party provider as an~~





~~enterprise information technology service~~. The provision of data center services must comply with applicable state and federal laws, regulations, and policies, including all applicable security, privacy, and auditing requirements. The department shall appoint a director of the state data center, preferably an individual who has experience in leading data center facilities and has expertise in cloud-computing management.

~~(1) INTENT.—The Legislature finds that the most efficient and effective means of providing quality utility data processing services to state agencies requires that computing resources be concentrated in quality facilities that provide the proper security, disaster recovery, infrastructure, and staff resources to ensure that the state's data is maintained reliably and safely, and is recoverable in the event of a disaster. Unless otherwise exempt by law, it is the intent of the Legislature that all agency data centers and computing facilities shall be consolidated into the state data center.~~

(1)~~(2)~~ STATE DATA CENTER DUTIES.—The state data center shall:

(a) Offer, develop, and support the services and applications defined in service-level agreements executed with its customer entities.

(b) Maintain performance of the state data center by ensuring proper data backup, data backup recovery, disaster recovery, and appropriate security, power, cooling, fire suppression, and capacity.

(c) Develop and implement ~~a~~ business continuity ~~plan~~ and ~~a~~ disaster recovery plans ~~plan, and beginning July 1, 2015~~, and annually ~~thereafter,~~ conduct a live exercise of each plan.

(d) Enter into a service-level agreement with each customer entity to provide the required type and level of service or services. If a customer entity fails to execute an agreement within 60 days after commencement of a service, the state data center may cease service. A service-level agreement may not have a term exceeding 3 years and at a minimum must:

1. Identify the parties and their roles, duties, and responsibilities under the agreement.

2. State the duration of the contract term and specify the conditions for renewal.

3. Identify the scope of work.

4. Identify the products or services to be delivered with sufficient specificity to permit an external financial or performance audit.

5. Establish the services to be provided, the business standards that must be met for each service, the cost of each service by agency application, and the metrics and processes by which the business standards for each service are to be objectively measured and reported.

6. Provide a timely billing methodology to recover the costs of services provided to the customer entity pursuant to s. 215.422.

7. Provide a procedure for modifying the service-level agreement based on changes in the type, level, and cost of a service.

8. Include a right-to-audit clause to ensure that the parties to the agreement have access to records for audit purposes during the term of the service-level agreement.

9. Provide that a service-level agreement may be terminated





by either party for cause only after giving the other party and the department ~~Agency for State Technology~~ notice in writing of the cause for termination and an opportunity for the other party to resolve the identified cause within a reasonable period.

10. Provide for mediation of disputes by the Division of Administrative Hearings pursuant to s. 120.573.

(e) For purposes of chapter 273, be the custodian of resources and equipment located in and operated, supported, and managed by the state data center.

(f) Assume administrative access rights to resources and equipment, including servers, network components, and other devices, consolidated into the state data center.

1. Upon ~~the date of each~~ consolidation ~~specified in this section, the General Appropriations Act, or any other law~~, a state agency shall relinquish administrative rights to consolidated resources and equipment. State agencies required to comply with federal and state criminal justice information security rules and policies shall retain administrative access rights sufficient to comply with the management control provisions of those rules and policies; however, the state data center shall have the appropriate type or level of rights to allow the center to comply with its duties pursuant to this section. The Department of Law Enforcement shall serve as the arbiter of disputes pertaining to the appropriate type and level of administrative access rights pertaining to the provision of management control in accordance with the federal criminal justice information guidelines.

2. The state data center shall provide customer entities with access to applications, servers, network components, and

other devices necessary for entities to perform business activities and functions, and as defined and documented in a service-level agreement.

(g) In its procurement process, show preference for cloud-computing solutions that minimize or do not require the purchasing, financing, or leasing of state data center infrastructure, and that meet the needs of customer agencies, that reduce costs, and that meet or exceed the applicable state and federal laws, regulations, and standards for information technology security.

(h) Assist customer entities in transitioning from state data center services to third-party cloud-computing services procured by a customer entity.

~~(3) STATE AGENCY DUTIES.—~~

~~(a) Each state agency shall provide to the Agency for State Technology all requested information relating to its data centers and computing facilities and any other information relevant to the effective transition of an agency data center or computing facility into the state data center.~~

~~(b) Each state agency customer of the state data center shall notify the state data center, by May 31 and November 30 of each year, of any significant changes in anticipated utilization of state data center services pursuant to requirements established by the state data center.~~

(2) ~~(4)~~ USE OF THE STATE DATA CENTER ~~SCHEDULE FOR CONSOLIDATIONS OF AGENCY DATA CENTERS~~.—

~~(a) Consolidations of agency data centers and computing facilities into the state data center shall be made by the dates specified in this section and in accordance with budget~~



**CODING:** Words ~~stricken~~ are deletions; words underlined are additions.



~~adjustments contained in the General Appropriations Act.~~

~~(b) During the 2013-2014 fiscal year, the following state agencies shall be consolidated by the specified date:~~

~~1. By October 31, 2013, the Department of Economic Opportunity.~~

~~2. By December 31, 2013, the Executive Office of the Governor, to include the Division of Emergency Management except for the Emergency Operation Center's management system in Tallahassee and the Camp Blanding Emergency Operations Center in Starke.~~

~~3. By March 31, 2014, the Department of Elderly Affairs.~~

~~4. By October 30, 2013, the Fish and Wildlife Conservation Commission, except for the commission's Fish and Wildlife Research Institute in St. Petersburg.~~

~~(c)~~ The following are exempt from the use of the state data center ~~consolidation under this section~~: the Department of Law Enforcement, the Department of the Lottery's Gaming System, Systems Design and Development in the Office of Policy and Budget, the regional traffic management centers as described in s. 335.14(2) and the Office of Toll Operations of the Department of Transportation, the State Board of Administration, state attorneys, public defenders, criminal conflict and civil regional counsel, capital collateral regional counsel, and the Florida Housing Finance Corporation.

~~(d) A state agency that is consolidating its agency data center or computing facility into the state data center must execute a new or update an existing service-level agreement within 60 days after the commencement of the service. If a state agency and the state data center are unable to execute a~~



**CODING:** Words ~~stricken~~ are deletions; words underlined are additions.

~~service-level agreement by that date, the agency shall submit a report to the Executive Office of the Governor within 5 working days after that date which explains the specific issues preventing execution and describing the plan and schedule for resolving those issues.~~

~~(c) Each state agency scheduled for consolidation into the state data center shall submit a transition plan to the Agency for State Technology by July 1 of the fiscal year before the fiscal year in which the scheduled consolidation will occur. Transition plans shall be developed in consultation with the state data center and must include:~~

~~1. An inventory of the agency data center's resources being consolidated, including all hardware and its associated life cycle replacement schedule, software, staff, contracted services, and facility resources performing data center management and operations, security, backup and recovery, disaster recovery, system administration, database administration, system programming, job control, production control, print, storage, technical support, help desk, and managed services, but excluding application development, and the agency's costs supporting these resources.~~

~~2. A list of contracts in effect, including, but not limited to, contracts for hardware, software, and maintenance, which identifies the expiration date, the contract parties, and the cost of each contract.~~

~~3. A detailed description of the level of services needed to meet the technical and operational requirements of the platforms being consolidated.~~

~~4. A timetable with significant milestones for the~~



**CODING:** Words ~~stricken~~ are deletions; words underlined are additions.



~~completion of the consolidation.~~

~~(f) Each state agency scheduled for consolidation into the state data center shall submit with its respective legislative budget request the specific recurring and nonrecurring budget adjustments of resources by appropriation category into the appropriate data processing category pursuant to the legislative budget request instructions in s. 216.023.~~

(3)~~(5)~~ AGENCY LIMITATIONS.—

~~(a)~~ Unless exempt from the use of the state data center ~~consolidation~~ pursuant to this section or authorized by the Legislature ~~or as provided in paragraph (b)~~, a state agency may not:

(a)~~1.~~ Create a new agency computing facility or data center, or expand the capability to support additional computer equipment in an existing agency computing facility or data center; or

~~2. Spend funds before the state agency's scheduled consolidation into the state data center to purchase or modify hardware or operations software that does not comply with standards established by the Agency for State Technology pursuant to s. 282.0051;~~

~~3. Transfer existing computer services to any data center other than the state data center;~~

(b)~~4.~~ Terminate services with the state data center without giving written notice of intent to terminate services 180 days before such termination~~; or~~

~~5. Initiate a new computer service except with the state data center.~~

~~(b) Exceptions to the limitations in subparagraphs (a)1.,~~



**CODING:** Words ~~stricken~~ are deletions; words underlined are additions.

~~2., 3., and 5. may be granted by the Agency for State Technology if there is insufficient capacity in the state data center to absorb the workload associated with agency computing services, if expenditures are compatible with the standards established pursuant to s. 282.0051, or if the equipment or resources are needed to meet a critical agency business need that cannot be satisfied by the state data center. The Agency for State Technology shall establish requirements that a state agency must follow when submitting and documenting a request for an exception. The Agency for State Technology shall also publish guidelines for its consideration of exception requests. However, the decision of the Agency for State Technology regarding an exception request is not subject to chapter 120~~.

Section 11. Section 282.206, Florida Statutes, is created to read:

282.206 Cloud-first policy in state agencies.—

(1) The Legislature finds that the most efficient and effective means of providing quality data processing services is through the use of cloud computing. It is the intent of the Legislature that each state agency adopt a cloud-first policy that first considers cloud-computing solutions in its technology sourcing strategy for technology initiatives or upgrades whenever possible and feasible.

(2) In its procurement process, each state agency shall show a preference for cloud-computing solutions that either minimize or do not require the use of state data center infrastructure when cloud-computing solutions meet the needs of the agency, reduce costs, and meet or exceed the applicable state and federal laws, regulations, and standards for





information technology security.

(3) Each state agency shall adopt formal procedures for the evaluation of cloud-computing options for existing applications, technology initiatives, or upgrades.

(4) Each state agency shall develop a strategic plan to be updated annually to address its inventory of applications located at the state data center. Each agency shall submit the plan by October 15 of each year to the Office of Policy and Budget in the Executive Office of the Governor and the chairs of the legislative appropriations committees. For each application, the plan must identify and document the readiness, appropriate strategy, and high-level timeline for transition to a cloud-computing service based on the application's quality, cost, and resource requirements. This information must be used to assist the state data center in making adjustments to its service offerings.

(5) Each state agency customer of the state data center shall notify the state data center by May 31 and November 30 annually of any significant changes in its anticipated utilization of state data center services pursuant to requirements established by the state data center.

(6) Unless authorized by the Legislature, the Department of Law Enforcement, as the state's lead Criminal Justice Information Services Systems Agency, may not impose more stringent protection measures than outlined in the federal Criminal Justice Information Services Security Policy relating to the use of cloud-computing services.

Section 12. Section 282.318, Florida Statutes, is amended to read:

282.318 Security of data and information technology.—

(1) This section may be cited as the "Information Technology Security Act."

(2) As used in this section, the term "state agency" has the same meaning as provided in s. 282.0041, except that the term includes the Department of Legal Affairs, the Department of Agriculture and Consumer Services, and the Department of Financial Services.

(3) The department ~~Agency for State Technology~~ is responsible for establishing standards and processes consistent with generally accepted best practices for information technology security, to include cybersecurity, and adopting rules that safeguard an agency's data, information, and information technology resources to ensure availability, confidentiality, and integrity and to mitigate risks. The department ~~agency~~ shall also:

(a) Designate a state chief information security officer who must have experience and expertise in security and risk management for communications and information technology resources.

(b) ~~(a)~~ Develop, and annually update by February 1, a statewide information technology security strategic plan that includes security goals and objectives for the strategic issues of information technology security policy, risk management, training, incident management, and disaster recovery planning.

(c) ~~(b)~~ Develop and publish for use by state agencies an information technology security framework that, at a minimum, includes guidelines and processes for:

1. Establishing asset management procedures to ensure that





an agency's information technology resources are identified and managed consistent with their relative importance to the agency's business objectives.

2. Using a standard risk assessment methodology that includes the identification of an agency's priorities, constraints, risk tolerances, and assumptions necessary to support operational risk decisions.

3. Completing comprehensive risk assessments and information technology security audits, which may be completed by a private sector vendor, and submitting completed assessments and audits to the department ~~Agency for State Technology~~.

4. Identifying protection procedures to manage the protection of an agency's information, data, and information technology resources.

5. Establishing procedures for accessing information and data to ensure the confidentiality, integrity, and availability of such information and data.

6. Detecting threats through proactive monitoring of events, continuous security monitoring, and defined detection processes.

7. Establishing agency computer security incident response teams and describing their responsibilities for responding to information technology security incidents, including breaches of personal information containing confidential or exempt data.

8. Recovering information and data in response to an information technology security incident. The recovery may include recommended improvements to the agency processes, policies, or guidelines.

9. Establishing an information technology security incident

reporting process that includes procedures and tiered reporting timeframes for notifying the department ~~Agency for State Technology~~ and the Department of Law Enforcement of information technology security incidents. The tiered reporting timeframes shall be based upon the level of severity of the information technology security incidents being reported.

10. Incorporating information obtained through detection and response activities into the agency's information technology security incident response plans.

11. Developing agency strategic and operational information technology security plans required pursuant to this section.

12. Establishing the managerial, operational, and technical safeguards for protecting state government data and information technology resources that align with the state agency risk management strategy and that protect the confidentiality, integrity, and availability of information and data.

(d) ~~(c)~~ Assist state agencies in complying with this section.

(e) ~~(d)~~ In collaboration with the Cybercrime Office of the Department of Law Enforcement, annually provide training for state agency information security managers and computer security incident response team members that contains training on information technology security, including cybersecurity, threats, trends, and best practices.

(f) ~~(e)~~ Annually review the strategic and operational information technology security plans of executive branch agencies.

(4) Each state agency head shall, at a minimum:

(a) Designate an information security manager to administer





the information technology security program of the state agency. This designation must be provided annually in writing to the department ~~Agency for State Technology~~ by January 1. A state agency's information security manager, for purposes of these information security duties, shall report directly to the agency head.

(b) In consultation with the department ~~Agency for State Technology~~ and the Cybercrime Office of the Department of Law Enforcement, establish an agency computer security incident response team to respond to an information technology security incident. The agency computer security incident response team shall convene upon notification of an information technology security incident and must comply with all applicable guidelines and processes established pursuant to paragraph (3)(c) ~~paragraph (3)(b)~~.

(c) Submit to the department ~~Agency for State Technology~~ annually by July 31, the state agency's strategic and operational information technology security plans developed pursuant to rules and guidelines established by the department ~~Agency for State Technology~~.

1. The state agency strategic information technology security plan must cover a 3-year period and, at a minimum, define security goals, intermediate objectives, and projected agency costs for the strategic issues of agency information security policy, risk management, security training, security incident response, and disaster recovery. The plan must be based on the statewide information technology security strategic plan created by the department ~~Agency for State Technology~~ and include performance metrics that can be objectively measured to

reflect the status of the state agency's progress in meeting security goals and objectives identified in the agency's strategic information security plan.

2. The state agency operational information technology security plan must include a progress report that objectively measures progress made towards the prior operational information technology security plan and a project plan that includes activities, timelines, and deliverables for security objectives that the state agency will implement during the current fiscal year.

(d) Conduct, and update every 3 years, a comprehensive risk assessment, which may be completed by a private sector vendor, to determine the security threats to the data, information, and information technology resources, including mobile devices and print environments, of the agency. The risk assessment must comply with the risk assessment methodology developed by the department ~~Agency for State Technology~~ and is confidential and exempt from s. 119.07(1), except that such information shall be available to the Auditor General, the Division of State Technology within the department ~~Agency for State Technology~~, the Cybercrime Office of the Department of Law Enforcement, and, for state agencies under the jurisdiction of the Governor, the Chief Inspector General.

(e) Develop, and periodically update, written internal policies and procedures, which include procedures for reporting information technology security incidents and breaches to the Cybercrime Office of the Department of Law Enforcement and the Division of State Technology within the department ~~Agency for State Technology~~. Such policies and procedures must be



consistent with the rules, guidelines, and processes established by the department ~~Agency for State Technology~~ to ensure the security of the data, information, and information technology resources of the agency. The internal policies and procedures that, if disclosed, could facilitate the unauthorized modification, disclosure, or destruction of data or information technology resources are confidential information and exempt from s. 119.07(1), except that such information shall be available to the Auditor General, the Cybercrime Office of the Department of Law Enforcement, the Division of State Technology within the department ~~Agency for State Technology~~, and, for state agencies under the jurisdiction of the Governor, the Chief Inspector General.

(f) Implement managerial, operational, and technical safeguards and risk assessment remediation plans recommended by the department ~~Agency for State Technology~~ to address identified risks to the data, information, and information technology resources of the agency.

(g) Ensure that periodic internal audits and evaluations of the agency's information technology security program for the data, information, and information technology resources of the agency are conducted. The results of such audits and evaluations are confidential information and exempt from s. 119.07(1), except that such information shall be available to the Auditor General, the Cybercrime Office of the Department of Law Enforcement, the Division of State Technology within the department ~~Agency for State Technology~~, and, for agencies under the jurisdiction of the Governor, the Chief Inspector General.

(h) Ensure that the ~~Include appropriate~~ information

technology security and cybersecurity requirements in both the written specifications for the solicitation and service-level agreement of information technology and information technology resources and services meet or exceed the applicable state and federal laws, regulations, and standards for information technology security and cybersecurity. Service-level agreements must identify service provider and state agency responsibilities for privacy and security, protection of government data, personnel background screening, and security deliverables with associated frequencies~~, which are consistent with the rules and guidelines established by the Agency for State Technology in collaboration with the Department of Management Services~~.

(i) Provide information technology security and cybersecurity awareness training to all state agency employees in the first 30 days after commencing employment concerning information technology security risks and the responsibility of employees to comply with policies, standards, guidelines, and operating procedures adopted by the state agency to reduce those risks. The training may be provided in collaboration with the Cybercrime Office of the Department of Law Enforcement.

(j) Develop a process for detecting, reporting, and responding to threats, breaches, or information technology security incidents which is consistent with the security rules, guidelines, and processes established by the Agency for State Technology.

1. All information technology security incidents and breaches must be reported to the Division of State Technology within the department ~~Agency for State Technology~~ and the Cybercrime Office of the Department of Law Enforcement and must





comply with the notification procedures and reporting timeframes established pursuant to paragraph (3)(c) ~~paragraph (3)(b)~~.

2. For information technology security breaches, state agencies shall provide notice in accordance with s. 501.171.

3. Records held by a state agency which identify detection, investigation, or response practices for suspected or confirmed information technology security incidents, including suspected or confirmed breaches, are confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution, if the disclosure of such records would facilitate unauthorized access to or the unauthorized modification, disclosure, or destruction of:

a. Data or information, whether physical or virtual; or

b. Information technology resources, which includes:

(I) Information relating to the security of the agency's technologies, processes, and practices designed to protect networks, computers, data processing software, and data from attack, damage, or unauthorized access; or

(II) Security information, whether physical or virtual, which relates to the agency's existing or proposed information technology systems.

Such records shall be available to the Auditor General, the Division of State Technology within the department ~~Agency for State Technology~~, the Cybercrime Office of the Department of Law Enforcement, and, for state agencies under the jurisdiction of the Governor, the Chief Inspector General. Such records may be made available to a local government, another state agency, or a federal agency for information technology security purposes or

in furtherance of the state agency's official duties. This exemption applies to such records held by a state agency before, on, or after the effective date of this exemption. This subparagraph is subject to the Open Government Sunset Review Act in accordance with s. 119.15 and shall stand repealed on October 2, 2021, unless reviewed and saved from repeal through reenactment by the Legislature.

(5) The portions of risk assessments, evaluations, external audits, and other reports of a state agency's information technology security program for the data, information, and information technology resources of the state agency which are held by a state agency are confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution if the disclosure of such portions of records would facilitate unauthorized access to or the unauthorized modification, disclosure, or destruction of:

(a) Data or information, whether physical or virtual; or

(b) Information technology resources, which include:

1. Information relating to the security of the agency's technologies, processes, and practices designed to protect networks, computers, data processing software, and data from attack, damage, or unauthorized access; or

2. Security information, whether physical or virtual, which relates to the agency's existing or proposed information technology systems.

Such portions of records shall be available to the Auditor General, the Cybercrime Office of the Department of Law Enforcement, the Division of State Technology within the





department ~~Agency for State Technology~~, and, for agencies under the jurisdiction of the Governor, the Chief Inspector General. Such portions of records may be made available to a local government, another state agency, or a federal agency for information technology security purposes or in furtherance of the state agency's official duties. For purposes of this subsection, "external audit" means an audit that is conducted by an entity other than the state agency that is the subject of the audit. This exemption applies to such records held by a state agency before, on, or after the effective date of this exemption. This subsection is subject to the Open Government Sunset Review Act in accordance with s. 119.15 and shall stand repealed on October 2, 2021, unless reviewed and saved from repeal through reenactment by the Legislature.

(6) The department ~~Agency for State Technology~~ shall adopt rules relating to information technology security and to administer this section.

Section 13. Subsections (1) and (2) of section 17.0315, Florida Statutes, are amended to read:

17.0315 Financial and cash management system; task force.—

(1) The Chief Financial Officer, as the constitutional officer responsible for settling and approving accounts against the state and keeping all state funds pursuant to s. 4, Art. IV of the State Constitution, is the head of and shall appoint members to a task force established to develop a strategic business plan for a successor financial and cash management system. The task force shall include the state chief information officer ~~executive director of the Agency for State Technology~~ and the director of the Office of Policy and Budget in the

Executive Office of the Governor. Any member of the task force may appoint a designee.

(2) The strategic business plan for a successor financial and cash management system must:

(a) Permit proper disbursement and auditing controls consistent with the respective constitutional duties of the Chief Financial Officer and the Legislature;

(b) Promote transparency in the accounting of public funds;

(c) Provide timely and accurate recording of financial transactions by agencies and their professional staffs;

(d) Support executive reporting and data analysis requirements;

(e) Be capable of interfacing with other systems providing human resource services, procuring goods and services, and providing other enterprise functions;

(f) Be capable of interfacing with the existing legislative appropriations, planning, and budgeting systems;

(g) Be coordinated with the information technology strategy development efforts of the Department of Management Services ~~Agency for State Technology~~;

(h) Be coordinated with the revenue estimating conference process as supported by the Office of Economic and Demographic Research; and

(i) Address other such issues as the Chief Financial Officer identifies.

Section 14. Paragraph (d) of subsection (1) of section 20.055, Florida Statutes, is amended to read:

20.055 Agency inspectors general.—

(1) As used in this section, the term:



(d) "State agency" means each department created pursuant to this chapter and the Executive Office of the Governor, the Department of Military Affairs, the Fish and Wildlife Conservation Commission, the Office of Insurance Regulation of the Financial Services Commission, the Office of Financial Regulation of the Financial Services Commission, the Public Service Commission, the Board of Governors of the State University System, the Florida Housing Finance Corporation, ~~the Agency for State Technology,~~ the Office of Early Learning, and the state courts system.

Section 15. Paragraph (b) of subsection (3) of section 97.0525, Florida Statutes, is amended to read:

97.0525 Online voter registration.—

(3)

(b) The division shall conduct a comprehensive risk assessment of the online voter registration system before making the system publicly available and every 2 years thereafter. The comprehensive risk assessment must comply with the risk assessment methodology developed by the Department of Management Services ~~Agency for State Technology~~ for identifying security risks, determining the magnitude of such risks, and identifying areas that require safeguards.

Section 16. Paragraph (e) of subsection (2) of section 110.205, Florida Statutes, is amended to read:

110.205 Career service; exemptions.—

(2) EXEMPT POSITIONS.—The exempt positions that are not covered by this part include the following:

(e) The state chief information officer ~~executive director of the Agency for State Technology~~. Unless otherwise fixed by

law, the Department of Management Services ~~Agency for State Technology~~ shall set the salary and benefits of this position in accordance with the rules of the Senior Management Service.

Section 17. Subsections (2) and (9) of section 215.322, Florida Statutes, are amended to read:

215.322 Acceptance of credit cards, charge cards, debit cards, or electronic funds transfers by state agencies, units of local government, and the judicial branch.—

(2) A state agency as defined in s. 216.011, or the judicial branch, may accept credit cards, charge cards, debit cards, or electronic funds transfers in payment for goods and services with the prior approval of the Chief Financial Officer. If the Internet or other related electronic methods are to be used as the collection medium, the state chief information officer ~~Agency for State Technology~~ shall review and recommend to the Chief Financial Officer whether to approve the request with regard to the process or procedure to be used.

(9) For payment programs in which credit cards, charge cards, or debit cards are accepted by state agencies, the judicial branch, or units of local government, the Chief Financial Officer, in consultation with the state chief information officer ~~Agency for State Technology~~, may adopt rules to establish uniform security safeguards for cardholder data and to ensure compliance with the Payment Card Industry Data Security Standards.

Section 18. Subsection (2) of section 215.96, Florida Statutes, is amended to read:

215.96 Coordinating council and design and coordination staff.—



**CODING:** Words ~~stricken~~ are deletions; words underlined are additions.



(2) The coordinating council shall consist of the Chief Financial Officer; the Commissioner of Agriculture; the Attorney General; the Secretary of Management Services; the state chief information officer ~~executive director of the Agency for State Technology~~; and the Director of Planning and Budgeting, Executive Office of the Governor, or their designees. The Chief Financial Officer, or his or her designee, shall be chair of the council, and the design and coordination staff shall provide administrative and clerical support to the council and the board. The design and coordination staff shall maintain the minutes of each meeting and make such minutes available to any interested person. The Auditor General, the State Courts Administrator, an executive officer of the Florida Association of State Agency Administrative Services Directors, and an executive officer of the Florida Association of State Budget Officers, or their designees, shall serve without voting rights as ex officio members of the council. The chair may call meetings of the council as often as necessary to transact business; however, the council shall meet at least once a year. Action of the council shall be by motion, duly made, seconded and passed by a majority of the council voting in the affirmative for approval of items that are to be recommended for approval to the Financial Management Information Board.

Section 19. Subsection (22) of section 287.057, Florida Statutes, is amended to read:

287.057 Procurement of commodities or contractual services.—

(22) The department, in consultation with the Chief Financial Officer and the state chief information officer ~~Agency~~



**CODING:** Words ~~stricken~~ are deletions; words underlined are additions.

~~for State Technology~~, shall maintain a program for online procurement of commodities and contractual services. To enable the state to promote open competition and leverage its buying power, agencies shall participate in the online procurement program, and eligible users may participate in the program. Only vendors prequalified as meeting mandatory requirements and qualifications criteria may participate in online procurement.

(a) The department~~, in consultation with the Agency for State Technology and in compliance with the standards of the agency,~~ may contract for equipment and services necessary to develop and implement online procurement.

(b) The department shall adopt rules to administer the program for online procurement. The rules must include, but not be limited to:

1. Determining the requirements and qualification criteria for prequalifying vendors.

2. Establishing the procedures for conducting online procurement.

3. Establishing the criteria for eligible commodities and contractual services.

4. Establishing the procedures for providing access to online procurement.

5. Determining the criteria warranting any exceptions to participation in the online procurement program.

(c) The department may impose and shall collect all fees for the use of the online procurement systems.

1. The fees may be imposed on an individual transaction basis or as a fixed percentage of the cost savings generated. At a minimum, the fees must be set in an amount sufficient to cover





the projected costs of the services, including administrative and project service costs in accordance with the policies of the department.

2. If the department contracts with a provider for online procurement, the department, pursuant to appropriation, shall compensate the provider from the fees after the department has satisfied all ongoing costs. The provider shall report transaction data to the department each month so that the department may determine the amount due and payable to the department from each vendor.

3. All fees that are due and payable to the state on a transactional basis or as a fixed percentage of the cost savings generated are subject to s. 215.31 and must be remitted within 40 days after receipt of payment for which the fees are due. For fees that are not remitted within 40 days, the vendor shall pay interest at the rate established under s. 55.03(1) on the unpaid balance from the expiration of the 40-day period until the fees are remitted.

4. All fees and surcharges collected under this paragraph shall be deposited in the Operating Trust Fund as provided by law.

Section 20. Section 282.00515, Florida Statutes, is amended to read:

282.00515 Duties of Cabinet agencies.—The Department of Legal Affairs, the Department of Financial Services, and the Department of Agriculture and Consumer Services shall adopt the standards established in s. 282.0051(2), (3), and (7) ~~s. 282.0051(2), (3), and (8)~~ or adopt alternative standards based on best practices and industry standards, and may contract with

the department ~~Agency for State Technology~~ to provide or perform any of the services and functions described in s. 282.0051 for the Department of Legal Affairs, the Department of Financial Services, or the Department of Agriculture and Consumer Services.

Section 21. Subsections (3) and (4) of section 287.0591, Florida Statutes, are amended to read:

287.0591 Information technology.—

(3) The department may execute a state term contract for information technology commodities, consultant services, or staff augmentation contractual services that exceeds the 48-month requirement if the Secretary of Management Services and the state chief information officer ~~executive director of the Agency for State Technology~~ certify to the Executive Office of the Governor that a longer contract term is in the best interest of the state.

(4) If the department issues a competitive solicitation for information technology commodities, consultant services, or staff augmentation contractual services, the Division of State Technology within the department ~~Agency for State Technology~~ shall participate in such solicitations.

Section 22. Paragraph (a) of subsection (3) of section 365.171, Florida Statutes, is amended to read:

365.171 Emergency communications number E911 state plan.—

(3) DEFINITIONS.—As used in this section, the term:

(a) "Office" means the Division of State Technology ~~Program~~ within the Department of Management Services, as designated by the secretary of the department.

Section 23. Paragraph (s) of subsection (3) of section





365.172, Florida Statutes, is amended to read:

365.172 Emergency communications number "E911."—

(3) DEFINITIONS.—Only as used in this section and ss. 365.171, 365.173, and 365.174, the term:

(s) "Office" means the Division of State Technology ~~Program~~ within the Department of Management Services, as designated by the secretary of the department.

Section 24. Paragraph (a) of subsection (1) of section 365.173, Florida Statutes, is amended to read:

365.173 Communications Number E911 System Fund.—

(1) REVENUES.—

(a) Revenues derived from the fee levied on subscribers under s. 365.172(8) must be paid by the board into the State Treasury on or before the 15th day of each month. Such moneys must be accounted for in a special fund to be designated as the Emergency Communications Number E911 System Fund, a fund created in the Division of State Technology ~~Program~~, or other office as designated by the Secretary of Management Services.

Section 25. Subsection (4) of section 445.011, Florida Statutes, is amended to read:

445.011 Workforce information systems.—

(4) CareerSource Florida, Inc., shall coordinate development and implementation of workforce information systems with the state chief information officer ~~executive director of the Agency for State Technology~~ to ensure compatibility with the state's information system strategy and enterprise architecture.

Section 26. Subsection (2) and paragraphs (a) and (b) of subsection (4) of section 445.045, Florida Statutes, are amended to read:

445.045 Development of an Internet-based system for information technology industry promotion and workforce recruitment.—

(2) CareerSource Florida, Inc., shall coordinate with the Department of Management Services ~~Agency for State Technology~~ and the Department of Economic Opportunity to ensure links, as feasible and appropriate, to existing job information websites maintained by the state and state agencies and to ensure that information technology positions offered by the state and state agencies are posted on the information technology website.

(4)(a) CareerSource Florida, Inc., shall coordinate development and maintenance of the website under this section with the state chief information officer ~~executive director of the Agency for State Technology~~ to ensure compatibility with the state's information system strategy and enterprise architecture.

(b) CareerSource Florida, Inc., may enter into an agreement with ~~the Agency for State Technology,~~ the Department of Economic Opportunity~~,~~ or any other public agency with the requisite information technology expertise for the provision of design, operating, or other technological services necessary to develop and maintain the website.

Section 27. Paragraph (b) of subsection (18) of section 668.50, Florida Statutes, is amended to read:

668.50 Uniform Electronic Transaction Act.—

(18) ACCEPTANCE AND DISTRIBUTION OF ELECTRONIC RECORDS BY GOVERNMENTAL AGENCIES.—

(b) To the extent that a governmental agency uses electronic records and electronic signatures under paragraph (a), the Department of Management Services ~~Agency for State~~



**CODING:** Words ~~stricken~~ are deletions; words underlined are additions.



~~Technology~~, in consultation with the governmental agency, giving due consideration to security, may specify:

1. The manner and format in which the electronic records must be created, generated, sent, communicated, received, and stored and the systems established for those purposes.

2. If electronic records must be signed by electronic means, the type of electronic signature required, the manner and format in which the electronic signature must be affixed to the electronic record, and the identity of, or criteria that must be met by, any third party used by a person filing a document to facilitate the process.

3. Control processes and procedures as appropriate to ensure adequate preservation, disposition, integrity, security, confidentiality, and auditability of electronic records.

4. Any other required attributes for electronic records which are specified for corresponding nonelectronic records or reasonably necessary under the circumstances.

Section 28. Subsections (4) and (5) of section 943.0415, Florida Statutes, are amended to read:

943.0415 Cybercrime Office.—There is created within the Department of Law Enforcement the Cybercrime Office. The office may:

(4) Provide security awareness training and information to state agency employees concerning cybersecurity, online sexual exploitation of children, and security risks, and the responsibility of employees to comply with policies, standards, guidelines, and operating procedures adopted by the department ~~Agency for State Technology~~.

(5) Consult with the Division of State Technology within



**CODING:** Words ~~stricken~~ are deletions; words underlined are additions.

the Department of Management Services ~~Agency for State Technology~~ in the adoption of rules relating to the information technology security provisions in s. 282.318.

Section 29. Florida Cybersecurity Task Force.—

(1) The Florida Cybersecurity Task Force, a task force as defined in s. 20.03(8), Florida Statutes, is created adjunct to the Department of Management Services to review and conduct an assessment of the state's cybersecurity infrastructure, governance, and operations. Except as otherwise provided in this section, the task force shall operate in a manner consistent with s. 20.052, Florida Statutes.

(2) The task force consists of the following members:

(a) The Lieutenant Governor, or his or her designee, who shall serve as chair of the task force.

(b) A representative of the computer crime center of the Department of Law Enforcement, appointed by the executive director of the department.

(c) A representative of the fusion center of the Department of Law Enforcement, appointed by the executive director of the department.

(d) The state chief information officer.

(e) The state chief information security officer.

(f) A representative of the Division of Emergency Management within the Executive Office of the Governor, appointed by the director of the division.

(g) A representative of the Office of the Chief Inspector General in the Executive Office of the Governor, appointed by the Chief Inspector General.

(h) An individual appointed by the President of the Senate.



(i) An individual appointed by the Speaker of the House of Representatives.

(j) Members of the private sector appointed by the Governor.

(3) The task force shall convene by October 1, 2019, and shall meet as necessary, but at least quarterly, at the call of the chair. The Division of State Technology within the Department of Management Services shall provide staffing and administrative support to the task force.

(4) The task force shall:

(a) Recommend methods to secure the state's network systems and data, including standardized plans and procedures to identify developing threats and to prevent unauthorized access and destruction of data.

(b) Identify and recommend remediation, if necessary, of high-risk cybersecurity issues facing state government.

(c) Recommend a process to regularly assess cybersecurity infrastructure and activities of executive branch agencies.

(d) Identify gaps in the state's overall cybersecurity infrastructure, governance, and current operations. Based on any findings of gaps or deficiencies, the task force shall make recommendations for improvement.

(e) Recommend cybersecurity improvements for the state's emergency management and disaster response systems.

(f) Recommend cybersecurity improvements of the state data center.

(g) Review and recommend improvements relating to the state's current operational plans for the response, coordination, and recovery from a cybersecurity attack.

(5) All executive branch departments and agencies shall cooperate fully with requests for information made by the task force.

(6) On or before November 1, 2020, the task force shall submit a final report of its findings and recommendations to the Governor, the President of the Senate, and the Speaker of the House of Representatives.

(7) This section expires January 1, 2021.

Section 30. This act shall take effect July 1, 2019.



**CODING:** Words ~~stricken~~ are deletions; words underlined are additions.


# Motorist Modernization Update

FEBRUARY 6, 2019

# Introduction

**The Motorist Modernization program will:**

- **Modernize driver license and vehicle registration systems to serve Florida's growing population, without growing government.**

**Phase I**
Total cost over 6 years – **$37M**

**Phase II**
Total cost over 6 years – **$39.5M**

Total projected cost for Phase I and Phase II – **$77M**

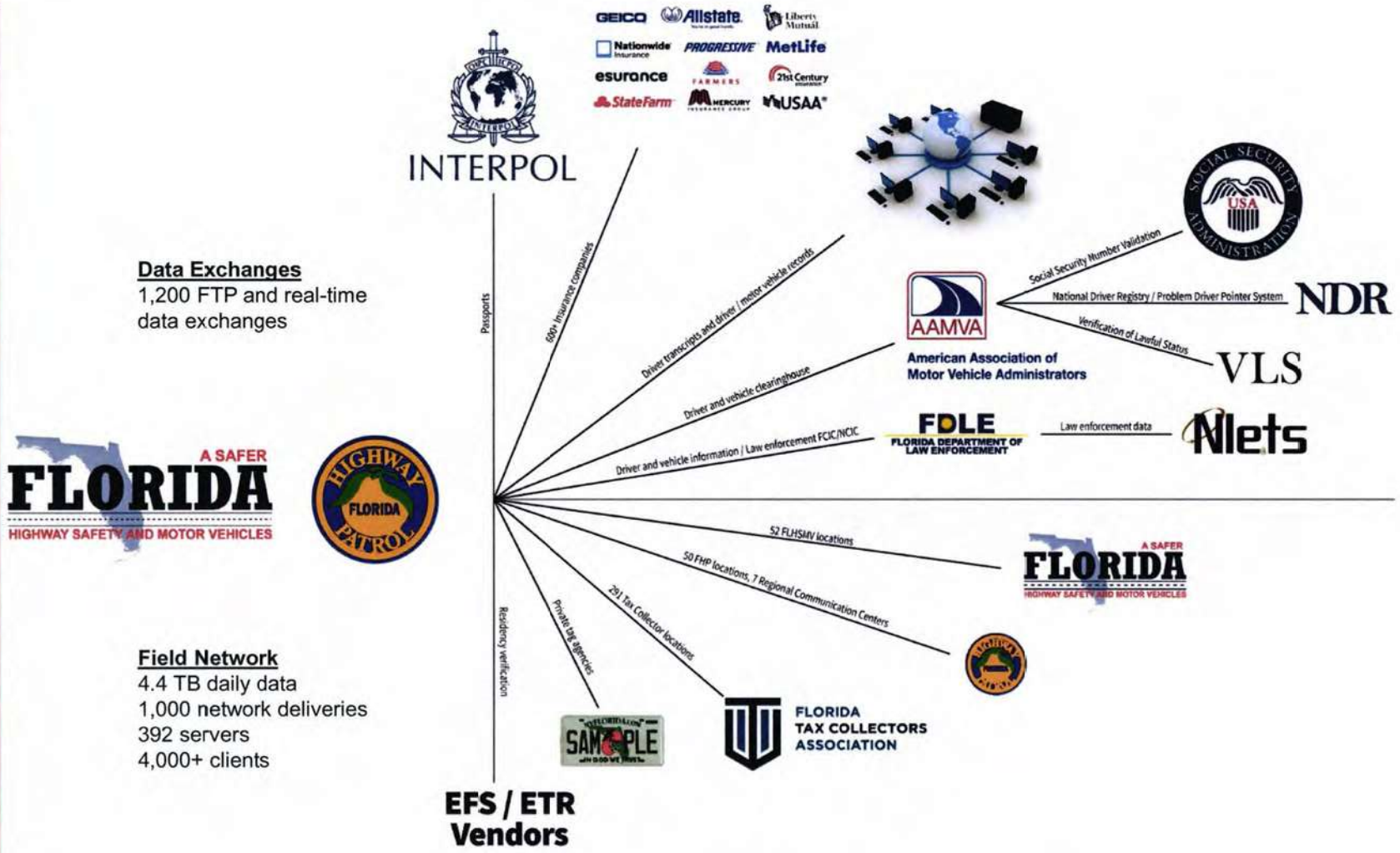
# Project Update

| | |
|---|---|
| Phase I Pilot | • Fiscal Year 19/20 Quarter 3 |
| Phase I Statewide Release | • Fiscal Year 19/20 Quarter 4 |
| Phase II Requirements Validation | • Fiscal Year 19/20 Quarter 1 |
| Phase II Commence Software Development | • Fiscal Year 19/20 Quarter 2 |

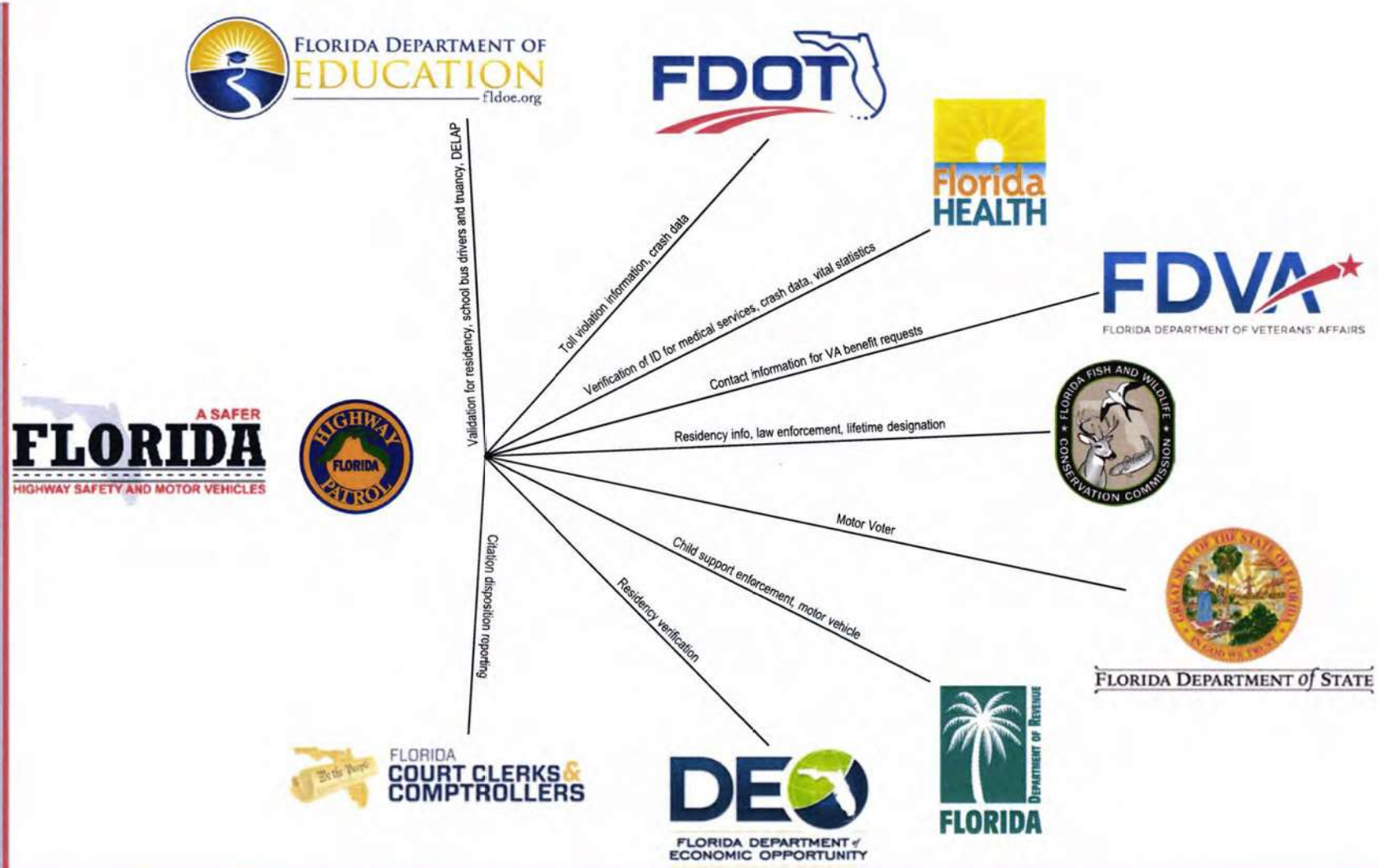
# Who Do We Connect With?

**Data Exchanges**
1,200 FTP and real-time data exchanges

**Field Network**
4.4 TB daily data
1,000 network deliveries
392 servers
4,000+ clients



# Data Exchanges with Other State Agencies



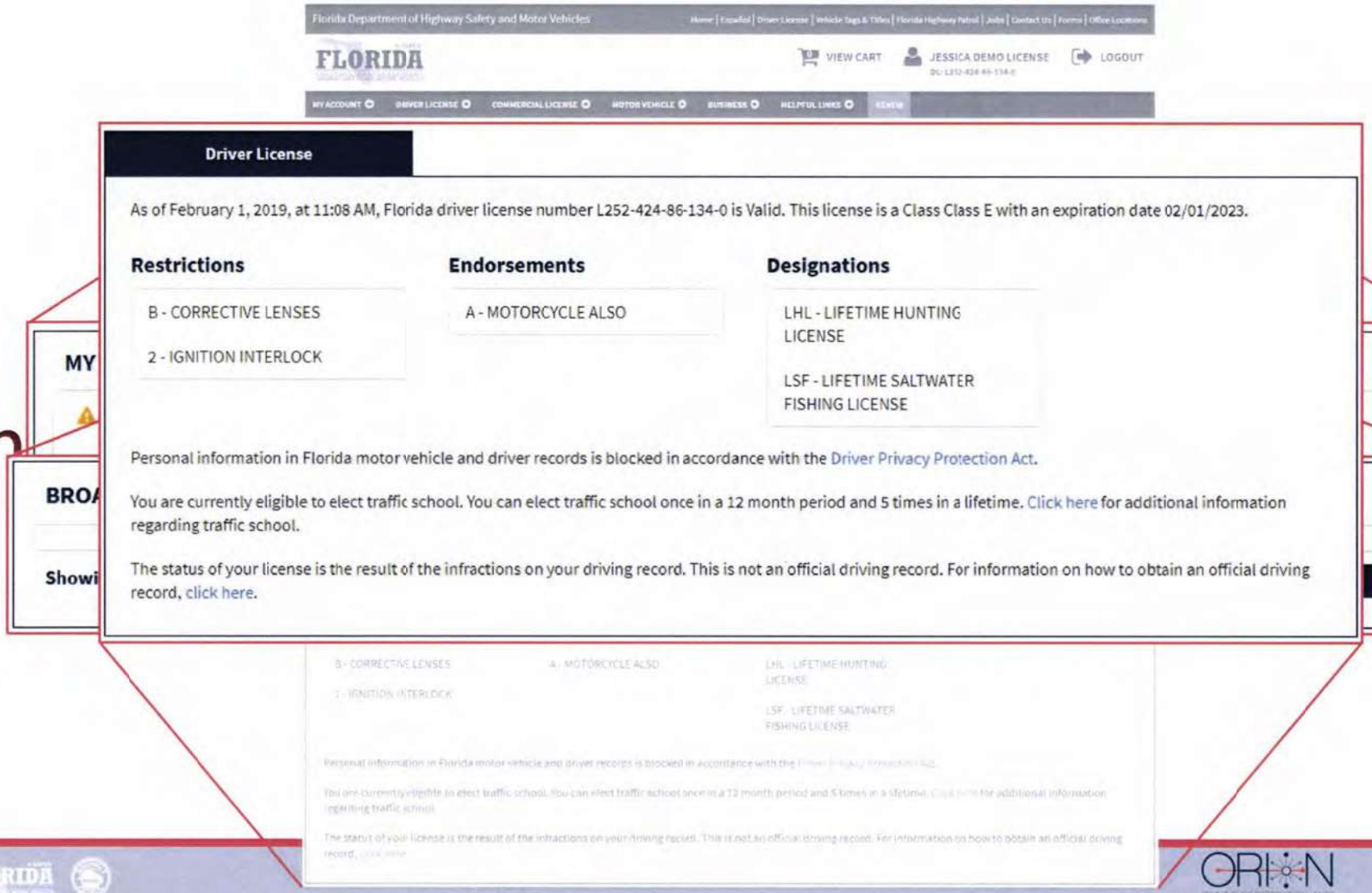
# Why the Modernization Effort Began

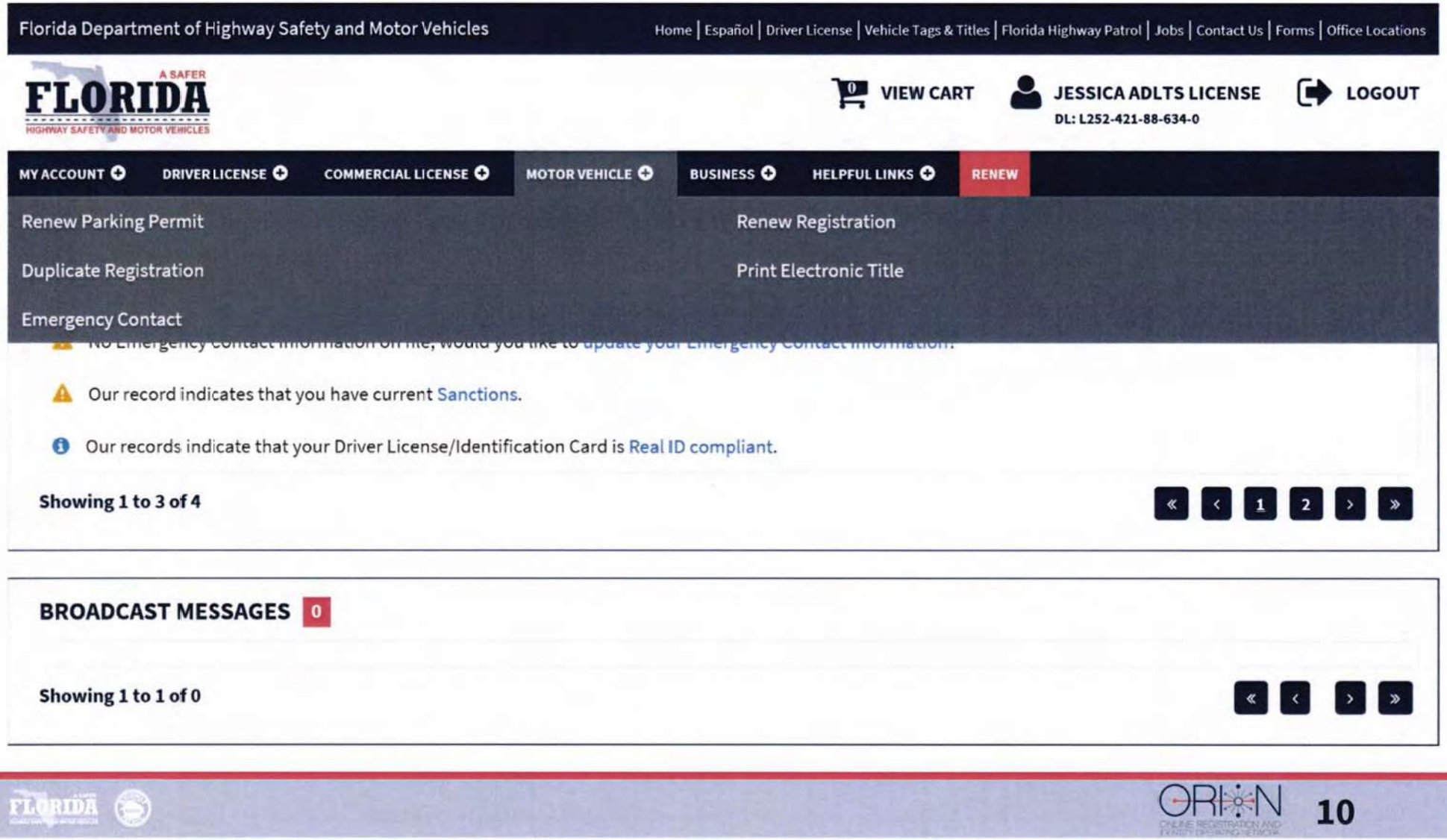
# Benefits

- Delivers a software system that is sustainable and scalable.
  - Mobile DL
  - Online Insurance Verification
- Enhances employee tools and work processes to strengthen the focus on customers and outcomes.
  - System checks to reduce user errors
  - Streamlined transaction workflow
- Enhances the department's ability to take advantage of cloud-computing services
- Reduces software development efforts by utilizing modern technology.
- Increases customer service and expands service delivery options.

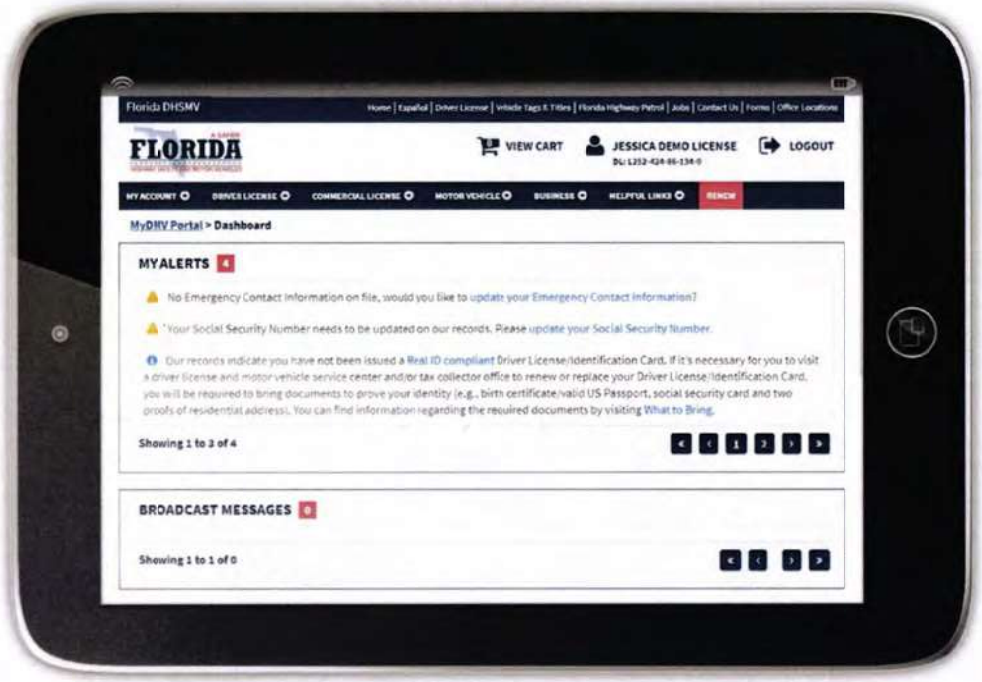
# MyDMV Portal Benefits

- Expands services to customers by providing the ability to clear certain sanctions online.
- Enables customers to subscribe to receive personalized alerts, as well as department notifications through the online portal.
- Provides businesses with new Commercial Driver License self-services online.
- Expands self-services for active duty military personnel online.


Florida Department of Highway Safety and Motor Vehicles
FLORIDA
VIEW CART
JESSICA DEMO LICENSE
LOGOUT
MY ACCOUNT
DRIVER LICENSE
COMMERCIAL LICENSE
MOTOR VEHICLE
BUSINESS
HELPFUL LINKS
Driver License
As of February 1, 2019, at 11:08 AM, Florida driver license number L252-424-86-134-0 is Valid. This license is a Class Class E with an expiration date 02/01/2023.
Restrictions
B - CORRECTIVE LENSES
2 - IGNITION INTERLOCK
Endorsements
A - MOTORCYCLE ALSO
Designations
LHL - LIFETIME HUNTING LICENSE
LSF - LIFETIME SALTWATER FISHING LICENSE
Personal information in Florida motor vehicle and driver records is blocked in accordance with the Driver Privacy Protection Act.
You are currently eligible to elect traffic school. You can elect traffic school once in a 12 month period and 5 times in a lifetime. Click here for additional information regarding traffic school.
The status of your license is the result of the infractions on your driving record. This is not an official driving record. For information on how to obtain an official driving record, click here.

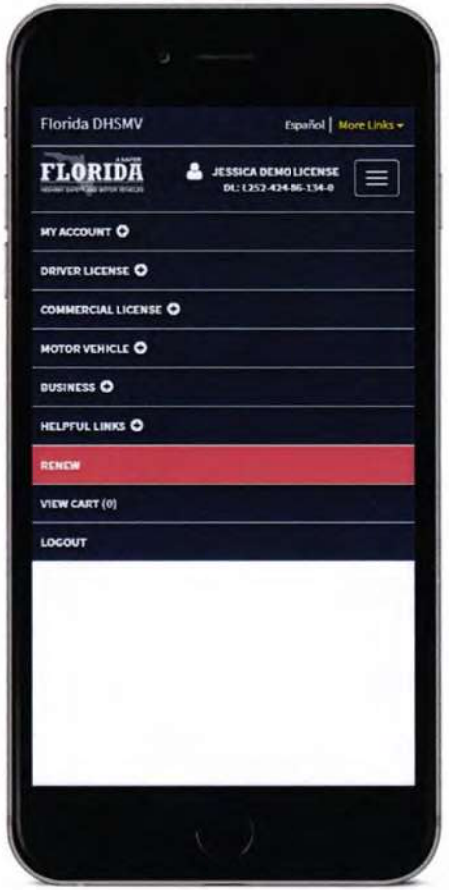

Florida Department of Highway Safety and Motor Vehicles
Home | Español | Driver License | Vehicle Tags & Titles | Florida Highway Patrol | Jobs | Contact Us | Forms | Office Locations
A SAFER FLORIDA
HIGHWAY SAFETY AND MOTOR VEHICLES
VIEW CART
JESSICA ADLTS LICENSE
DL: L252-421-88-634-0
LOGOUT
MY ACCOUNT
DRIVER LICENSE
COMMERCIAL LICENSE
MOTOR VEHICLE
BUSINESS
HELPFUL LINKS
RENEW
Renew Parking Permit
Renew Registration
Duplicate Registration
Print Electronic Title
Emergency Contact
Our record indicates that you have current Sanctions.
Our records indicate that your Driver License/Identification Card is Real ID compliant.
Showing 1 to 3 of 4
BROADCAST MESSAGES 0
Showing 1 to 1 of 0

Tablet View

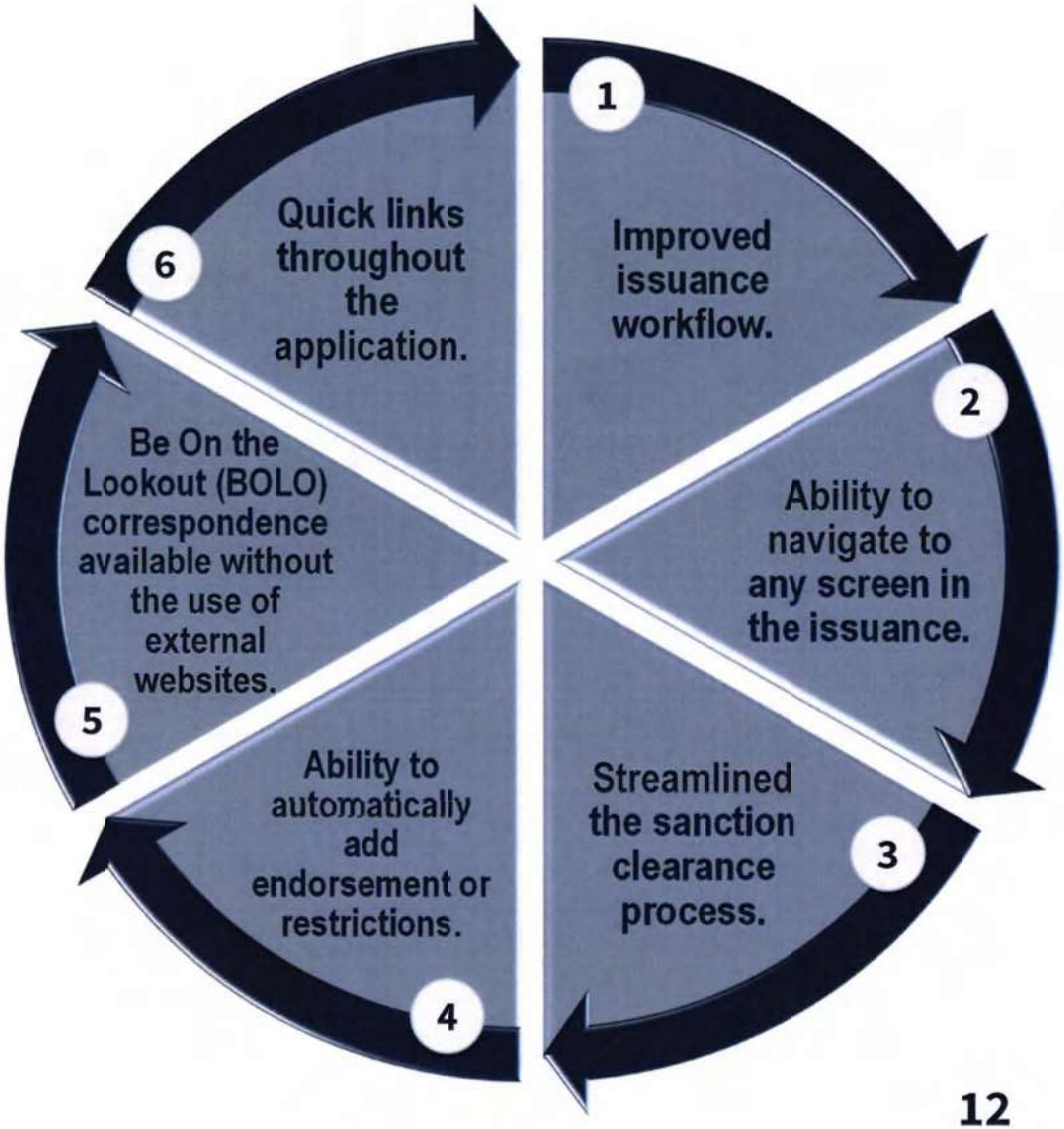



# MyDMV Portal

Mobile Phone View

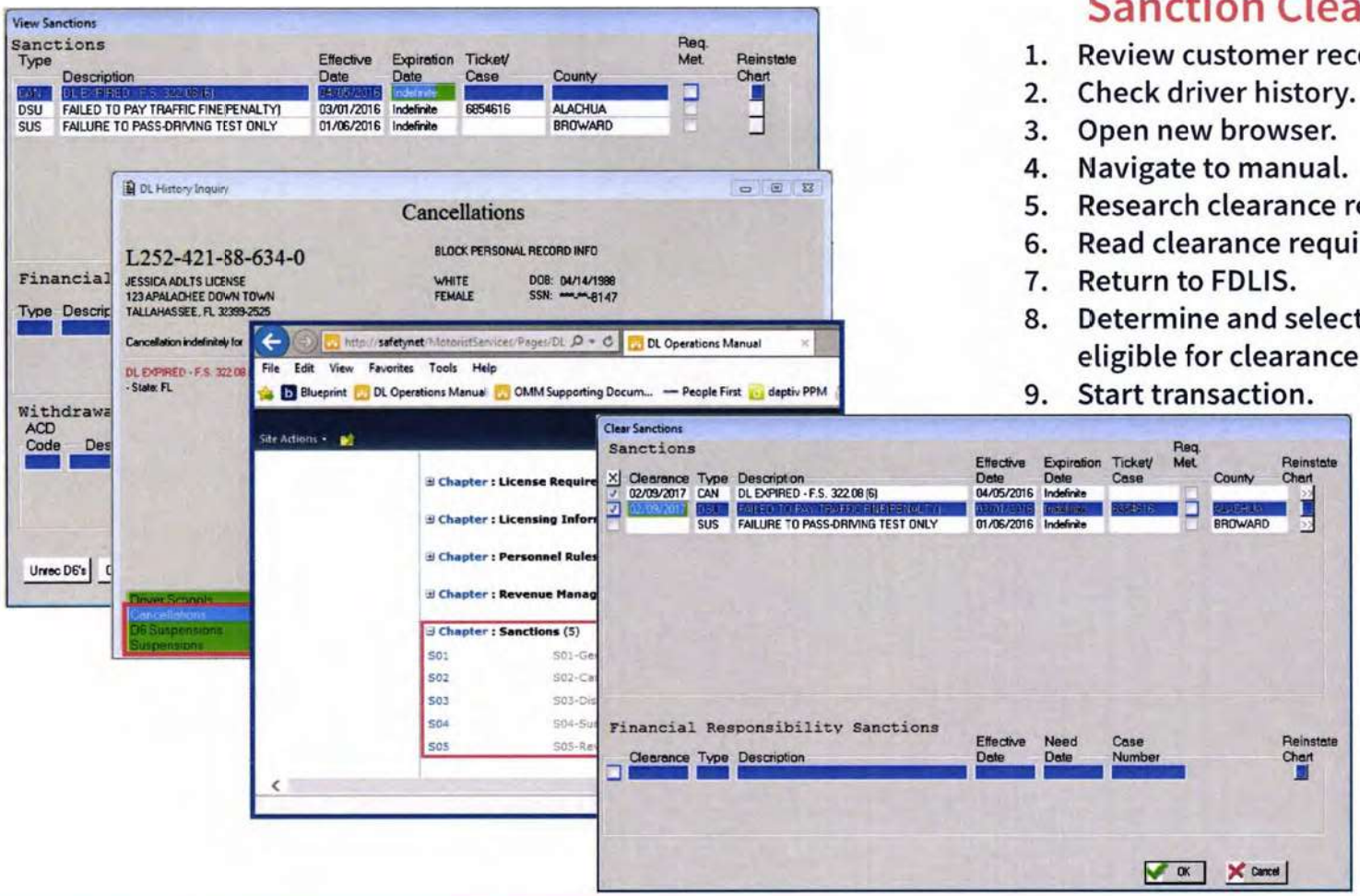


# System Enhancements for In Office Transactions



# System Enhancements for In Office Transactions

- Provide additional information to support expedited completion of motor vehicle transactions.
- Ability to pause transactions to expedite customer service.
- Linking transactions to simplify customer transaction workflow.

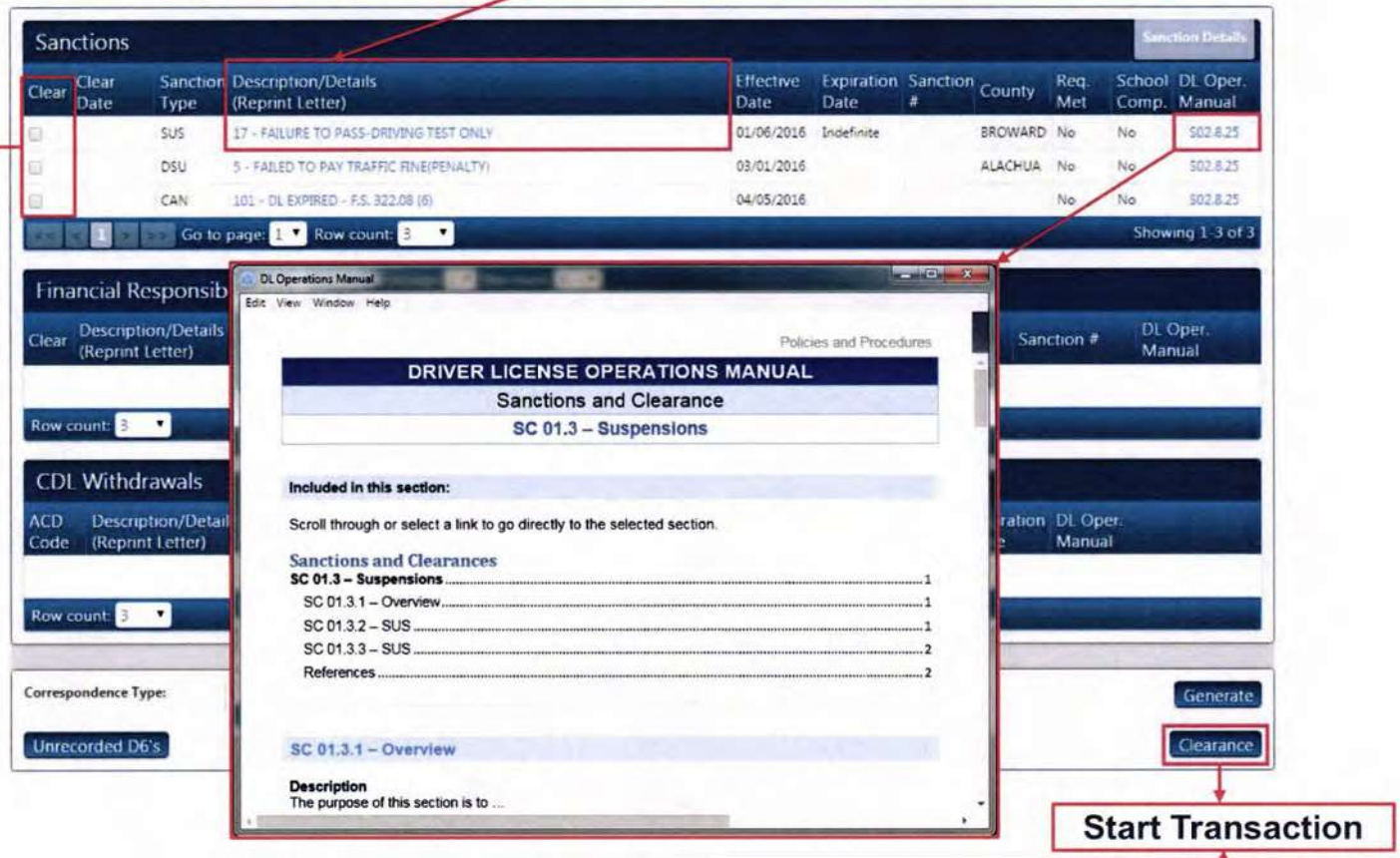



## Sanction Clearance

1. Review customer record.
2. Check driver history.
3. Open new browser.
4. Navigate to manual.
5. Research clearance requirements.
6. Read clearance requirements.
7. Return to FDLIS.
8. Determine and select sanctions eligible for clearance.
9. Start transaction.

# Motorist Modernization New System

**Navigates user to document mailed to customer with clearance instructions.**




# Questions?

A SAFER FLORIDA
HIGHWAY SAFETY AND MOTOR VEHICLES

ORION
ONLINE REGISTRATION AND IDENTITY OPERATING NETWORK


MotoristModernization@flhsmv.gov

# Proposal to Move the Florida Safe Families Network Application to a Cloud Computing Service


**October 30, 2015**

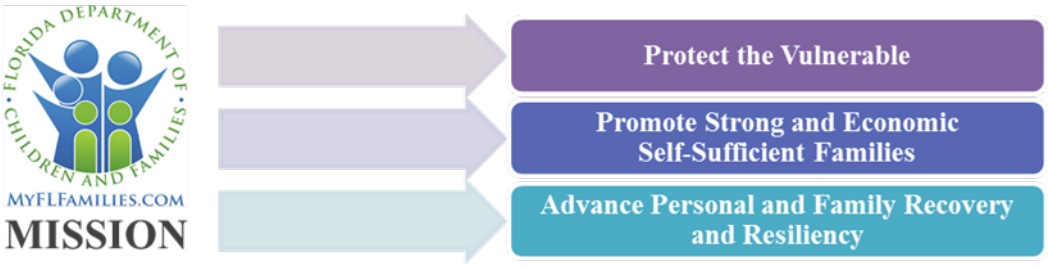
**DEPARTMENT OF CHILDREN AND FAMILIES**

# Table of Contents

# A. Executive Summary

## 1. Background

The Department of Children and Families (DCF or the Department) affects the lives of Floridians at times when their needs are greatest. The mission of the Department is to work in partnership with local communities to protect the vulnerable, promote strong and economically self-sufficient families, and advance personal and family recovery and resiliency.




**FSFN Mission Statement**

In 2005, Florida completed a transition to a Community Based Care (CBC) child welfare model, outsourcing case management services to private providers in local communities. With this new service delivery model, the Legislature found it critical to implement a statewide information system to ensure the consistent delivery of child welfare services across the state of Florida. The Florida Legislature established the Florida Safe Families Network (FSFN) in partnership with the federal Children's Bureau as the state's official Statewide Automated Child Welfare Information System (SACWIS). FSFN is the single information repository for all child welfare casework containing 30 years of data for over 8,000,000 people. Used by 15,000 child welfare professionals and partners, FSFN is Florida's comprehensive and systematic information technology solution to managing the care of at-risk children and family members.

FSFN is comprised of two distinct applications: the FSFN Case Management System and the Abuse Hotline Portal. The FSFN Case Management System is the primary application used by DCF, the Community Based Care organizations (CBCs) and other partners. It is a custom application that uses a SAP Business Objects data warehouse built to support Florida's unique child welfare practice. The FSFN Case Management System interfaces with the Abuse Hotline Portal used by the public and the DCF Abuse Hotline Call Center.

In accordance with the requirements outlined in the Fiscal Year 2015/2016 Budget, the Department is submitting this proposal outlining the costs and services necessary to support the FSFN development, test, user acceptance, and production environments in a commercial cloud environment. This proposal describes the:

- Types of cloud computing services available and considered for hosting FSFN;
- Cost benefit analysis for moving FSFN to a cloud service provider, including disaster recovery support;
- Benefits of moving FSFN to a cloud service provider, including disaster recovery support;
- Federal regulations and/or approvals needed for FSFN to reside in the cloud; and
- An implementation plan for migrating FSFN to the cloud by June 30, 2017.

As DCF considered the opportunity to leverage the benefits of the cloud, the as-is technical environment and business constraints were fully considered such that the provided proposal is both feasible and capable of supporting the availability, scalability, and recoverability requirements of the system.

The entire FSFN System is a highly customized web based application developed to meet Florida's needs. The

application is comprised of over 2,000 feature-rich screens that provide users the ability to initiate and manage cases, investigations, adoptions, placements, services, Medicaid and much more. A robust reporting system that provides a standardized data structure for creating custom reports, as well as standardized daily, weekly and monthly reports, supports these functions. The application also has multiple interfaces that export and import data with other systems such as the FLORIDA System, the Juvenile Justice Information System, Agency for Health Care Administration (AHCA) databases and the federal Children's Bureau.

FSFN is a multi-tier system that separates the web, application and data layers. This architecture enhances security and optimization of performance. This is critical given the sensitivity of the data that resides in the system and the need to process the data quickly. FSFN runs on mainframe and middle tier servers. The mainframe hosts a DB2 Database that holds over 30 years of child welfare data. The FLORIDA System shares this mainframe and utilizes approximately 70% of the overall data capacity, leaving FSFN with the remaining 30%. The remainder of the system (the web and application services) operate on Intel based middle tier servers. The entire application resides on 57 servers that run the application, reporting, interfaces and other system features.

A new FSFN portal was implemented (the Florida Abuse Hotline) in November 2012, replacing a system that had been in operation for decades, and introduced numerous new capabilities that improved the Department's responsiveness to child abuse reporting. This portal project also upgraded the Florida Abuse Hotline. The Florida Abuse Hotline integrates the call-taking, data analysis and investigation preparation activities into a seamless business operation. In 2013, the Department deployed major FSFN releases to implement safety methodology tools for investigations and case management. New functionality included at-a-glance views of case and person information, case notes enhancements, improved workflow and task assignment functions and new assessment tools—such as the Present Danger Assessment and Family Functioning Assessment—which are fundamental to Florida's new child welfare practice model. The revised Child Welfare Safety Methodology Practice Model and the technology that supports it are the foundation for the Department to achieve the goals of safe, permanent, and healthy children and families. FSFN enables the Child Welfare Safety Methodology Practice Model by providing the information technology platform for knowledge sharing and critical decision-making.

However, those incrementally deployed features and functions, built on existing legacy technical platforms from 2005, are not able to incorporate emerging application architectures and technologies, leaving the system at risk for failure to maintain supported platforms.

## 2. Cloud Hosting Comparison Approach

In order to define cloud hosting options and valid costs to incorporate into this proposal, DCF adopted the elements of a commercial grade cloud solution as the baseline model for the determination of cloud provider costs. Core hardware, software and service elements of the cloud solution baseline that are included in the costs outlined in this proposal include:

- Concurrently maintainable site infrastructure with expected availability of 99.95%
- High operational and performance requirements, metrics and penalties when metrics are not satisfied
- Full disaster recovery environment and testing with hardware availability in 24 hours and 36 hour recovery to a fully operational and available state
- Properly sized and scalable hardware and software environments based on transactional and operation usage requirements

The core elements, defined above, and the detail elements of the commercial cloud solution described in subsequent sections of this proposal, contribute significantly to the costs outlined.

When considering the commercial model and the current AST model, material differences between the two environments exist. This is particularly true for each of the core elements listed previously. For that reason, an analysis of AST service and cost differences between the proposed cloud and the current AST based solution is required to determine quantitative benefits. Since that analysis has not yet been undertaken, a cost benefits based comparison between the two solutions could not be defined. However, the proposal outlines the qualitative benefits of the proposed cloud solution.

## 3. Cloud Hosting Benefits and Options

Moving the FSFN System to a cloud service provider has inherent benefits over the current operational model. The benefits of a cloud based solution that employs cross-platform hosting of FSFN on a mainframe and on middle tier servers include:

- Greater operational capacity and flexibility as a result of on-demand hardware and software capabilities
- Unused capacity is not billed
- Defined and Enforceable Service Level Agreements (SLAs) for FSFN hosting with monetary penalties to mitigate operational risks
- Significantly enhanced disaster recovery capabilities for the replication of the application and data from the primary site to a recovery site. This allows the ability to recover FSFN within 36 hours at a "warm" recovery site. The current disaster recovery plan available for the FSFN System is a "cold" recovery site where backup tapes are sent to the site for a targeted 108-hour recovery.
- Improved hardware, software, and storage scalability for the support of and anticipated capacity requirements for the next 3-5 years based on current growth trends and functionality
- The agility and flexibility of an external hosting provider can improve system performance by adding capacity and addressing and resolving performance issues rapidly
- Dedicated resources supporting the system increases availability and reliability
- Hardware upgrades are included in the hosting costs
- Reduction to operation risks related to capacity expansion timeframes, disaster recovery, application support

DCF's expectation is that the cloud hosting service provider in partnership with the Agency for State Technology (AST) delivers a solution that has redundant network and storage paths in addition to server components to mitigate any single point of failure issues, including redundant active capacity components and distribution paths, concurrent maintenance, fault tolerance, compartmentalization and continuous cooling.

DCF considered three cloud-hosting alternatives: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). The National Institute of Standards and Technology (NIST) defines the three alternatives for cloud hosting as follows:

- **Alternative 1 - Software as a Service (SaaS)**

  For this option, cloud providers install and operate application software in the cloud. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g, web-based email), or program interface. The consumer does not manage or control the underlying cloud infrastructure including individual application capabilities, the network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user specific application configuration settings.

- **Alternative 2 - Platform as a Service (PaaS)**

  The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications developed using programming languages, libraries, services and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

- **Alternative 3 - Infrastructure as a Service (IaaS)**

  The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over the operating system, storage, deployed applications and possibly limited control of select networking components (e.g., host firewalls).

DCF performed a detailed assessment of the various options for hosting FSFN in the cloud. The approach consisted of assessing feasible options for different types of cloud hosting, identification of the current Agency for State Technology (AST) costs and costs to provide cloud hosting for FSFN using a mainframe, as well as an option to provide cloud hosting for FSFN by replacing the mainframe with mid-tier servers.

Based on this assessment, the conclusions are as follows:

- Qualitative benefits for migrating FSFN to the cloud are substantial and significantly different between a cloud hosting solution and the present solution at AST.
- Infrastructure as a Service (IaaS) provides the most viable cloud services option for the needs of FSFN. Infrastructure as a Service (IaaS) requires the least amount of effort and cost to move FSFN to a cloud service provider. Using an IaaS allows for FSFN to be migrated to like hardware without the need for a high level of modification to the application.
- The other two service models for cloud hosting, Platform as a Service and Software as a Service, require a high level of modification to the current FSFN application.
- The Implementation Plan must incorporate the required Federal Risk and Authorization Management Program Assessment.

## 4. Infrastructure Options for Cloud Hosting

Once Infrastructure as a Service (IaaS) was determined to be the desired cloud-hosting model, DCF considered the hosting infrastructure requirements that would comprise the IaaS environment. The current FSFN System uses a hybrid/blended infrastructure model where the mainframe supports the DB2 data layer and mid-tier servers support the web, application and reporting layers. DCF considered two infrastructure options:

- Option 1: “Hybrid/Blended” – A mainframe is used for the application transactional database (data layer), and middle tier servers are used for the rest of the infrastructure. This is the current architecture of the FSFN System.
- Option 2: “Mid-Tier” – All features migrate off the mainframe and FSFN runs strictly on middle tier servers.

DCF determined that Option 1 (Hybrid/Blended) and Option 2 (Mid-Tier) were both feasible because they could meet the Legislature’s completion goal of June 30, 2017. They also meet the qualitative goals of security, service level and disaster recovery. An analysis of the costs for the two feasible options was performed using hosting, staffing, migration and disaster recovery as evaluation criteria. The hosting costs include those costs required to provide the physical infrastructure (e.g., server hardware, networking, facility, HVAC, connectivity, rack space, storage, and bandwidth). The staffing costs include the labor to support the infrastructure (e.g., maintenance, operations, backups, monitoring, security, and management). The migration costs include those costs necessary to adapt the FSFN System applications (e.g.,design, development, testing, and deployment) to the cloud. The Disaster Recovery (DR) costs include those costs necessary to establish a Continuity of Operations Plan (COOP), provide a physical DR location, operate the transfer of data to mirror data from the primary production location to the DR production location and exercise an annual DR test to validate capability.

### Option 1: Hybrid/Blended Hosting

Migrating FSFN to a cloud service provider using a hybrid/blended server configuration (mainframe for the data layer and mid-tier servers for the web, application, and reporting layers) is one cloud-hosting option. This infrastructure model is similar to that presently used by FSFN. The analysis starts with Fiscal Year 2016/2017, with the expectation of procuring cloud services to start April 2016. The cost analysis includes the costs for cloud services, application support, disaster recovery, migration and a transition cost for the AST to maintain FSFN while migrating to the cloud. As evidenced by the data, the first year costs are significantly higher than future year costs due to one-time costs for the migration and transition of FSFN to the cloud. The table below provides a summary of the anticipated yearly costs for Option 1.

| Hybrid/Blended Hosting Option | FY 16/17 (last 6 months) | FY 17/18 | FY 18/19 | FY 19/20 | FY 20/21 | Total |
|---|---|---|---|---|---|---|
| **Cloud Service Provider - With Mainframe** | $3,850,404.43 | $4,208,352.13 | $4,165,913.27 | $4,189,239.20 | $4,213,386.56 | $20,627,295.59 |
| **Disaster Recovery** | $849,232.93 | $1,676,474.50 | $1,638,604.71 | $1,628,454.39 | $1,640,048.23 | $7,432,814.76 |
| **Migration - Cloud Prerequisite (Services)** | $2,851,200.00 | N/A | N/A | N/A | N/A | $2,851,200.00 |
| **Networking** | $351,120.00 | $152,120.00 | $152,120.00 | $152,120.00 | $152,120.00 | $959,600.00 |
| **Recurring - Application Support Services** | $2,000,000.00 | $2,750,000.00 | $3,000,000.00 | $3,000,000.00 | $2,750,000.00 | $13,500,000.00 |
| **Recurring - AST indirect costs*** | N/A | $644,086.00 | $644,086.00 | $644,086.00 | $644,086.00 | $2,576,344.00 |
| **AST Cost for Migration and Transition** | $3,711,219.39 | N/A | N/A | N/A | N/A | $3,711,219.39 |
| **Total** | $13,613,176.75 | $9,431,032.63 | $9,600,723.98 | $9,613,899.59 | $9,399,640.79 | $51,658,473.74 |

**Estimated based on Fiscal Year 2015/2016 Costs*

**Cloud Service Provider Costs for Hybrid/Blended Hosting for Fiscal Year 2016/2017 through Fiscal Year 2020/2021**

### Option 2: Mid-Tier Hosting

Migrating FSFN to a cloud service provider using middle tier servers only is the second option considered. The analysis starts with Fiscal Year 2016/2017, with the expectation of procuring cloud services to start April, 2016. The analysis includes the costs of moving FSFN off the mainframe, cloud services, application support, disaster recovery, migration and transition costs for the AST to maintain FSFN while migrating to the cloud. As evidenced by the data, the first year costs are significantly higher than future year costs due to one-time costs for the migration and transition of FSFN to the cloud. Included in the first year costs are the costs to migrate the data and the DB2 database application from the mainframe to the mid-tier servers. The table on the next page provides a summary of the anticipated yearly costs for the Alternative 2: Mid-Tier Hosting Option.

| Mid-Tier Hosting Option | FY 16/17 (last 6 months) | FY 17/18 | FY 18/19 | FY 19/20 | FY 20/21 | Total |
|---|---|---|---|---|---|---|
| **Cloud Service Provider - Without Mainframe** | $2,378,888.92 | $1,540,412.08 | $1,482,370.84 | $1,509,184.95 | $1,536,907.80 | $8,447,764.59 |
| **Disaster Recovery** | $593,206.21 | $553,519.45 | $525,843.73 | $535,310.41 | $544,998.40 | $2,752,878.20 |
| **Migration – Replatform Mainframe to Mid-Tier** | $2,043,200.00 | N/A | N/A | N/A | N/A | $2,043,200.00 |
| **Migration - Cloud Prerequisite (Services)** | $2,851,200.00 | N/A | N/A | N/A | N/A | $2,851,200.00 |
| **Networking** | $351,120.00 | $152,120.00 | $152,120.00 | $152,120.00 | $152,120.00 | $959,600.00 |
| **Recurring - Application Support Services** | $2,000,000.00 | $2,750,000.00 | $3,000,000.00 | $3,000,000.00 | $2,750,000.00 | $13,500,000.00 |
| **Recurring - AST Indirect Costs*** | N/A | $644,086.00 | $644,086.00 | $644,086.00 | $644,086.00 | $2,576,344.00 |
| **AST Cost for Migration and Transition** | $3,612,819.39 | N/A | N/A | N/A | N/A | $3,612,819.39 |
| **Total** | $13,830,434.52 | $5,640,137.53 | $5,804,420.57 | $5,840,701.36 | $5,628,112.20 | $36,743,806.18 |

**Estimated based on Fiscal Year 2015/2016 Costs*

**Cloud Service Provider Costs for Middle Tier Hosting for Fiscal Year 2016/2017 through Fiscal Year 2020/2021**

[THIS SPACE LEFT BLANK INTENTIONALLY]

## 5. Recommended Infrastructure Model and Benefits

The DCF analysis of the two alternatives concluded that the Option 2: Mid-Tier hosting offered the greatest economic value to DCF and the lowest long term total cost of ownership. The Option 2: Mid-Tier hosting resulted in a total cost of $37M versus Option 1: Hybrid/Blended hosting total costs of $52M through Fiscal Year 2020/2021.

| Service | AST Baseline FY 15/16 | External Cloud Provider Option – Current FSFN Hardware and Software Architecture (Average Annual Cost) | External Cloud Provider Option – Conversion off Mainframe to Full Mid-Tier (Average Annual Cost) |
|---|---|---|---|
| **External Cloud Provider – Cloud Hosting** | N/A | $ 4,048,637.98 | $ 1,558,648.35 |
| **External Cloud Provider – Staffing** | N/A | $ 2,708,333.33 | $ 2,708,333.33 |
| **External Cloud Provider – Disaster Recovery** | N/A | $ 1,514,122.61 | $ 505,055.81 |
| **Network Connection to Cloud Provider** | N/A | $ 152,120.00 | $ 152,120.00 |
| **AST Hosting (Current)** | $ 2,596,747.30 | N/A | N/A |
| **AST Staffing (Current)** | $ 704,563.36 | N/A | N/A |
| **AST Disaster Recovery (Current)** | $ 311,508.73 | N/A | N/A |
| **Total** | **$ 3,612,819.39** | **$ 8,423,213.92** | **$ 4,924,157.49** |

**Cost Comparison of Hosting Options**

## 6. Comparison Factors

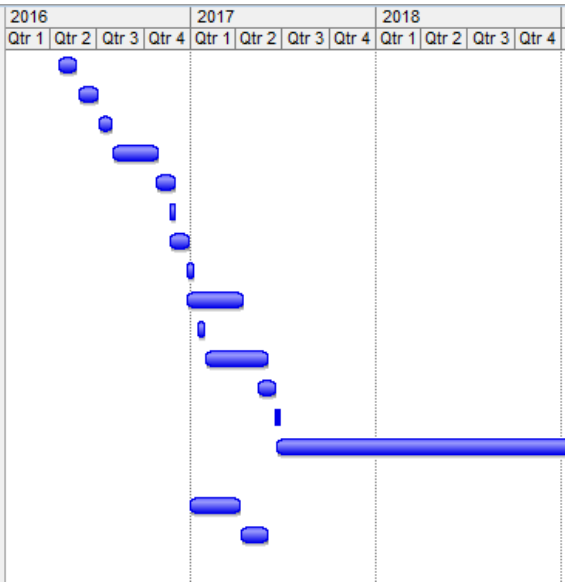
Key areas of comparison for a cost benefit analysis include Hosting, Staffing and Disaster Recovery Costs. The cost analysis for keeping the FSFN System with the AST includes the current Fiscal Year 2015/2016 as a baseline for AST charges to DCF specific to FSFN System. There are expected cost adjustments for AST starting in Fiscal Year 2016/2017 to account for a new mainframe lease, which includes additional capacity for FSFN and the FLORIDA System. There are expected cost adjustments starting in Fiscal Year 2017/2018 to include increased costs for new hardware for FSFN related to a hardware refresh and updating the application to operate on the most current versions of software platforms.

A comparison of the summary of costs for the two options above (1. IaaS with Mainframe and 2. IaaS without Mainframe), as well as the existing 2015/2016 AST costs to host FSFN are provided.

## 7. Project Plan

An evaluation of the options considering cost and hosting alternatives indicates that the FSFN migration to the cloud is feasible with an estimated schedule of 62 weeks. A project launch of April 16, 2016, with successful conclusion before June 30, 2017, is included in the plan.

| | Task Name | Start | Finish | Duration |
|---|---|---|---|---|
| 1 | FSFN Planning & Prerequisites | 4/15/2016 | 5/20/2016 | 4.55 wks |
| 2 | Contract & Budget Approved | 5/23/2016 | 7/1/2016 | 5.45 wks |
| 3 | Project Initiated | 7/1/2016 | 7/29/2016 | 3.64 wks |
| 4 | Development Ready for Migration | 7/29/2016 | 10/28/2016 | 11.82 wks |
| 5 | Development Migrated to Cloud | 10/24/2016 | 12/2/2016 | 5.45 wks |
| 6 | Test Ready for Migration | 11/18/2016 | 12/2/2016 | 1.82 wks |
| 7 | Test Migrated to Cloud | 11/21/2016 | 12/30/2016 | 5.45 wks |
| 8 | UAT Ready for Migration | 12/23/2016 | 1/6/2017 | 1.82 wks |
| 9 | UAT Migrated to Cloud | 12/23/2016 | 4/14/2017 | 14.55 wks |
| 10 | Production Ready for Migration | 1/13/2017 | 1/27/2017 | 1.82 wks |
| 11 | Production Operational | 1/30/2017 | 6/2/2017 | 16.36 wks |
| 12 | Proceed with Go Live | 5/12/2017 | 6/16/2017 | 4.55 wks |
| 13 | All Environments Migrated | 6/16/2017 | 6/23/2017 | 0.91 wks |
| 14 | Ongoing Support | 6/19/2017 | 7/1/2022 | 239.09 wks |
| 15 | | | | |
| 16 | Supported Platforms Testing | 12/30/2016 | 4/7/2017 | 12.73 wks |
| 17 | Supported Platforms Deployment | 4/10/2017 | 6/2/2017 | 7.27 wks |




**High Level Implementation Plan**

The Implementation Plan is key to managing the execution of the cloud migration and it leverages the established project management practices already in use by DCF. These include the current Governance, Deployment Procedures, Change Management and Risk Mitigation procedures.

It is important to note that a prerequisite to migrating the FSFN System to a cloud service provider is the version upgrades of the FSFN software platforms. The original plan was to perform that upgrade over a three-year period. However, the upgrades need to be completed prior to the migration to the cloud. In order to accommodate that requirement, the upgrade to supported platforms must be compressed to 18 months. The cost to perform this upgrade is included in the analysis of the first year costs.

## 8. Conclusion

DCF performed a detailed assessment of the various options for hosting FSFN in the cloud. The approach consisted of assessing feasible options for different types of cloud hosting. We identified the current Agency for State Technology (AST) costs and assessed costs to provide cloud hosting options for FSFN. A commercial option has potential benefits that may not be offered by a non-commercial hosting provider, such as a mechanism to enforce service levels through monetary penalties.

The DCF analysis of the two options concluded that the Mid-Tier hosting option offered the greatest economic value to DCF and the lowest long-term total cost of ownership with a cost of $37M through Fiscal Year 2020/2021. DCF also examined a second option, Hybrid/Blended, where a mainframe is used for the application transactional database (data layer), and middle tier servers are used for the rest of the infrastructure. This option resulted in a total cost of ownership with a cost of $52M through Fiscal Year 2020/2021. These total costs of ownership include the one-time costs to move FSFN to the cloud.

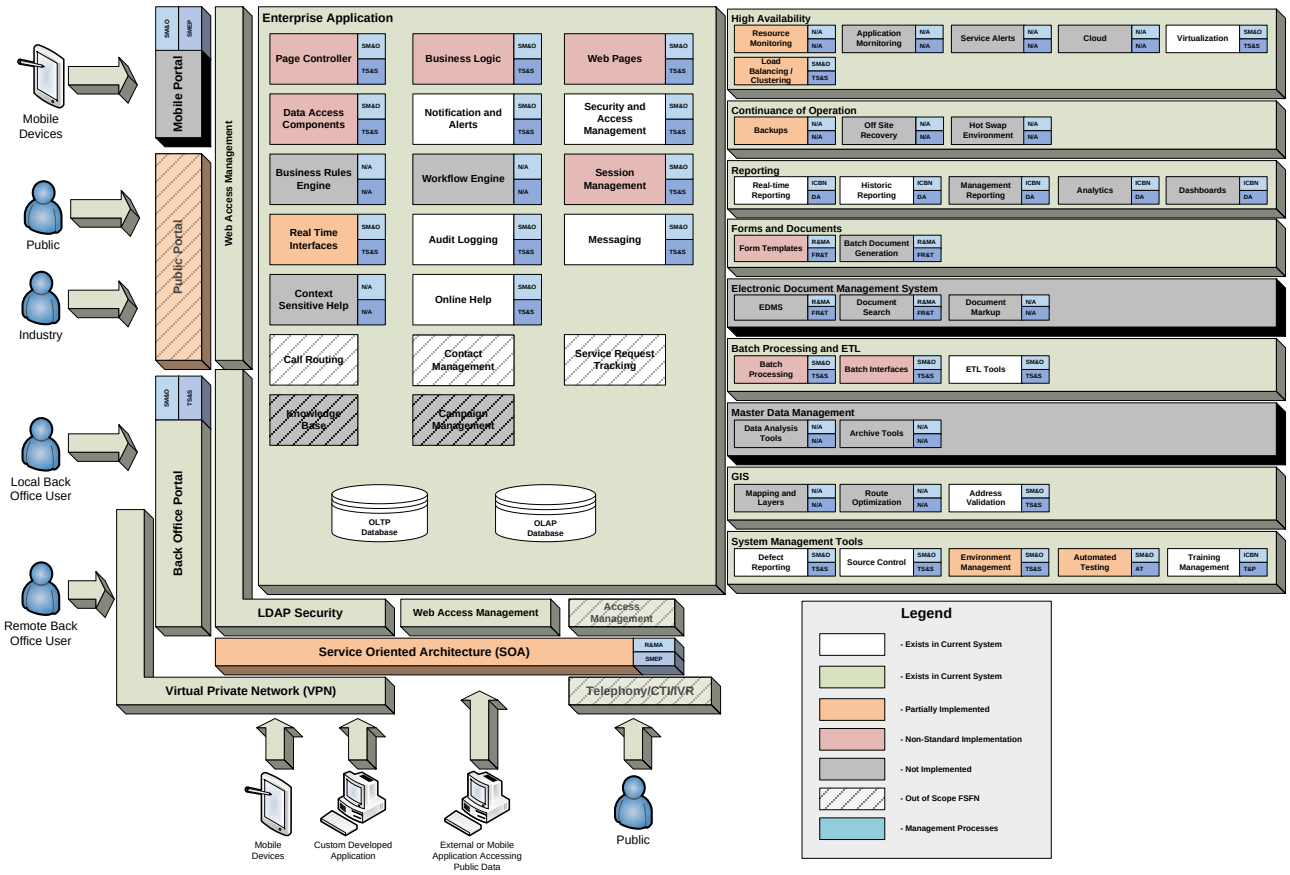
## B. Florida Safe Families Network (FSFN) System Overview

The Florida Safe Families Network (FSFN) System is the Florida's Statewide Automated Child Welfare Information System (SACWIS). The system is employed by over 15,000 users across the state. This user base is comprised of case workers, service providers, law enforcement and other partners that provide services for children in the state. Given the mission critical nature of the services performed, high availability and high reliability are essential.

The FSFN System is comprised of two distinct applications: the FSFN Case Management system and the Abuse Hotline Portal. The FSFN Case Management System is the primary application used by DCF, the CBCs and other partners. It is a custom application with an SAP Business Objects data warehouse that was built to support the State of Florida's unique child welfare environment. The second system, the Abuse Hotline Portal, is integrated closely with the FSFN Case Management System. The Abuse Hotline Portal is built on the Microsoft Dynamics platform and used by the public and the DCF Abuse Reporting Call Center.

The FSFN System (both Case Management and Portal) is web based, highly customized, adapted to the State of Florida's needs and comprises over 2,000 feature-rich screens. These screens provide users with the ability to initiate and manage cases, investigations, adoptions, placements, services, Medicaid, and much more. A robust reporting system that provides a standardized data structure for the creation of custom reports, as well as standardized daily, weekly, and monthly reports, supports these functions. There are multiple interfaces that export and import data with other systems such as the FLORIDA system, the Juvenile Justice Information System, the Agency for Health Care Administration (AHCA, and the federal Children's Bureau.

FSFN is a multi-tier system that separates the web, application and data layers. This architecture enables high security and optimization of system performance. FSFN runs on a mixture of mainframe and middle tier servers. The mainframe hosts a DB2 Database that holds over 30 years of Florida Child Welfare data. Currently, the mainframe is shared with the FLORIDA system, which utilizes approximately 70% of the overall capacity, leaving FSFN with the remaining 30%. The remainder of the system (the web and application services) operates on Intel based middle tier servers. There are 57 servers (across all environments) that provide the hardware for running the application, reporting, interfaces and other features of the system. The following diagram is a high-level view of the architecture of the Production Environment for FSFN and illustrates the breadth and depth of the FSFN application.




**FSFN System Architecture Overview**

## C. Definition of Cloud Service Provider and Fit for the FSFN System

When discussing cloud computing services for this plan, the definition of cloud computing utilized by the National Institute of Standards and Trainings (NIST) of the U.S. Department of Commerce will be used. The NIST definition characterizes important aspects of cloud computing and is intended to serve as a means for broad comparisons of cloud services and deployment strategies. It also provides a baseline for discussions ranging from a definition of cloud computing to how to best use cloud services.

According to the NIST definition, cloud computing has five essential characteristics, three service models, and four deployment models. Each of these items were considered in evaluating the options for a cloud service provider for FSFN.

The five essential characteristics of a cloud service that span all service and deployment models are:

| | |
|---|---|
| **On-Demand Self Service:** | Means that a customer can unilaterally provision computing capabilities (e.g., server time and network storage) automatically, as needed, without requiring human interaction with each service provider. |
| **Broad Network Access:** | Capabilities are available over the network and accessed through standard mechanisms that promote heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations). |
| **Resource Pooling:** | The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources (e.g., virtual machines, storage, or network) but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory and network bandwidth. |
| **Rapid Elasticity:** | Capabilities can be elastically (rapidly adding or removing virtual machines, processors, memory, or storage) provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time. |
| **Measured Service:** | Cloud systems automatically control and optimize resource use by leveraging a metering capability (ability to track usage, activity, or other infrastructure related metric) at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth and active user accounts). Resource usage can be monitored, controlled and reported, providing transparency for both the provider and consumer of the utilized service. |

The following are the service models that the NIST allows in the definition of cloud service:

| | |
|---|---|
| **Software as a Service (SaaS):** | The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g, web-based email), or program interface. The consumer does not manage or control the underlying cloud infrastructure including individual application capabilities, network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user specific application configuration settings. |
| **Platform as a Service (PaaS):** | The capability provided to the consumer is to deploy onto the Cloud infrastructure consumer-created or acquired applications developed using programming languages, libraries, services and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. |
| **Infrastructure as a Service (IaaS):** | The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating system, storage and deployed applications, and possibly limited control of select networking components (e.g., host firewalls). |

The following are the deployment models that the NIST allows in the definition of cloud service:

| | |
|---|---|
| **Private Cloud** | The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed and operated by the organization, a third party or some combination of them, and it may exist on or off premises |
| **Community Cloud** | The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy and compliance considerations). It may be owned, managed and operated by one or more of the organizations in the community, a third party or some combination of them, and it may exist on or off premises |
| **Public Cloud** | The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed and operated by one or more of a business, academic or government organization or some combination of them. It exists on the premises of the cloud services provider |
| **Hybrid Cloud** | The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds) |

Using the above NIST definition for cloud service, an analysis was performed on the characteristics, service model

and deployment models for evaluating a cloud service provider for FSFN.

Of the three service models for a cloud service, there are two models that do not meet the current needs of FSFN. The first is Software as a Service (SaaS) which is defined as using the provider's application. This would mean finding software that provides the same capabilities as FSFN and configuring the application to meet the needs of the users. Moving FSFN to a SaaS provider would entail a high degree of effort to convert existing legacy data to the new system, configure the system and test the entire system.

The other service model that does not meet the current needs of FSFN is Platform as a Service (PaaS). PaaS is defined as the service providing the programming languages, libraries, services and tools. FSFN has over eight years of custom code developed on specific software platforms and has specific needs in terms of programming languages, libraries, services and tools. Most PaaS providers do not have all of the platforms currently used in FSFN. There would be a high degree of effort to modify FSFN to function on the available software platforms, convert data to fit the new platforms and conduct a large testing effort of the entire system.

Infrastructure as a Service (IaaS) is the last of the service models and is the best fit for FSFN. Infrastructure as a Service is defined as the service providing processing, storage, networking and other fundamental computing resources. IaaS would allow the migration of FSFN, in its entirety, to a cloud services provider. The primary effort for moving FSFN is installing the required platforms, migrating code and data and testing the system functionality. This effort is significantly less than the effort associated with Software or Platform as a Service models.

When considering the four deployment models for cloud services, the primary considerations are the types of data stored in FSFN and access controls for the system and data. FSFN has different types of data with specific security needs, including personally identifiable information (PII), Personal Health Information (PHI), Health Information Portability and Accountability Act (HIPAA), Criminal Justice Information (CJI) and Medicaid data.

The deployment models for Public and Hybrid Clouds present a high degree of risk for FSFN. By definition, a Public Cloud involves sharing infrastructure and services with a range of clients that most likely will have disparate security needs. The range of clients and security needs increases exposure and the risk of compromising data security. For the same reason, a Hybrid Cloud, which includes a Public Cloud as part of the hybrid, inherits the same potential risk. This makes Public and Hybrid Clouds less of a fit for the security needs of FSFN.

The remaining two deployment models are Private and Community Cloud. The Private Cloud is an acceptable deployment model for the FSFN system because it provisions an infrastructure specifically for the customer. Provisioning the infrastructure allows the proper security controls to be put in place for protecting the system's data. Likewise, a Community Cloud is provisioned to meet the needs of a specific community, for example the federal government. In both cases, it is possible to find a service that meets the needs of FSFN.

The table on the next page provides a deeper analysis of the service models described in the NIST definition of cloud service.

| | PaaS (Platform) | SaaS (Software) | IaaS (Infrastructure) |
|---|---|---|---|
| **Considerations Related to Moving FSFN to a Specific Service** | | | |
| Software/Platform needs for hosting FSFN at a specific service | The service needs to provide Red Hat Enterprise Linux and Windows as operating systems. It needs to provide Oracle Web Logic, SAP Business Objects, SAP Data Services and Microsoft Dynamics as software platforms. It needs to provide Microsoft SQL Server and IBM DB2 for databases. | The Service needs to provide an application that functions as a Statewide Automated Child Welfare Information System (SACWIS). This application needs to support the specific functions needed by DCF, as well as providing capabilities for reports and interfaces. | The Service needs to provide like infrastructure (virtual machines, servers, storage, and network) to the current FSFN structure. |
| Modifications to FSFN needed for hosting FSFN at a specific service | If the service does not have a matching software platform to those used in FSFN, then areas of FSFN will need to be rewritten to allow the system to function on the provided platforms. | All FSFN functionality will need to be configured into the supported application. Reports would need to be modified to work in the supported application. Interfaces would need to be modified to work in the supported application. | As a prerequisite for hosting, all software platforms and supporting source code needs to be remediated to mainstream supported levels. This is needed to reduce support risks for the system after the system is migrated to the cloud. |
| Additional system preparation for migrating FSFN to a specific service | Build and test data conversion programs to migrate legacy data, historical reports, audit logs and user security to be accessible from the available platforms. | Build and test data conversion programs to migrate legacy data, historical reports, audit log, and user security to be accessible from the provided software. The provided software may not support some features that users may need historic access to. | Install software platforms used by FSFN. Copy data and deploy code. |

| | **PaaS (Platform)** | **SaaS (Software)** | **IaaS (Infrastructure)** |
|---|---|---|---|
| Testing effort needed to support migrating FSFN to a specific service | Full regression testing from both the application team and the end users, using existing test scripts. | Creation of new test scripts for all functionality in the system. Full regression testing from both the application team and end users. | Full regression testing from the application team, using existing test scripts. |
| Training effort needed to support migrating FSFN to a specific service | Training materials will need to be modified to accommodate changes in the software platform. All end users will need training for all changes. For example, if reporting capabilities were moved from Business Objects to Oracle Business Intelligence, then the users would need to be trained in the new tool. | All training materials will need to be rewritten to support the new software. All users of the system would need to be trained in the new software. | All existing training materials remain valid, and no additional training is necessary. |
| Limitations to expand the capabilities of FSFN for a specific service | Limited ability to expand the capabilities of the system by introducing new software platforms. For example, if DCF decided to replace a custom form with an Adobe product, the hosting service would need to offer Adobe as an available platform. | Limited to the functionality supplied in the provided software application. Desired features may not be available. | Limited to the ability of selected software to be installed and execute on a provided virtual machine. |
| **Responsibilities after FSFN Is Moved to a Specific Service** | | | |
| Hardware Monitoring | Service | Service | Service |
| Network Monitoring | Service | Service | Service |
| Application Monitoring | Service | Service | DCF |
| Operating System Monitoring | Service | Service | Service |
| Antivirus | Service | Service | Service |
| Server Patching | Service | Service | Service |

| | **PaaS (Platform)** | **SaaS (Software)** | **IaaS (Infrastructure)** |
|---|---|---|---|
| Operating System Patching | Service | Service | Service |
| Connectivity to FSFN from DCF | AST | AST | DCF |
| Software Install/Patching | Service | Service | DCF |
| Code Migrations | Service | Service | DCF |
| Physical DBA | Service | Service | AST |
| Logical DBA | Service | Service | DCF |
| Software Platform Support for Non-OS and Database | Service | Service | DCF |
| Defect Remediation | DCF | Service | DCF |
| System Enhancement | DCF | DCF/Service | DCF |
| Backups | Service | Service | Service |
| Disaster Recovery | Service | Service | DCF |
| Governance | DCF and Stakeholders | DCF and Stakeholders | DCF and Stakeholders |
| Training | DCF | DCF | DCF |
| Contract Management | AST | AST | AST |
| Contract Monitoring (SLAs) | DCF | DCF | DCF |
| Incident Management | DCF | DCF | DCF |
| Network Security | Service | Service | Service |
| Application Security | Service | Service | DCF |
| User Security | DCF | DCF | DCF |
| Facility Security | Service | Service | Service |
| Storage Security | Service | Service | Service |

In summary, FSFN is a complex system that utilizes multiple software platforms to provide the functions needed by the Department and its partners to perform day to day activities. Based on the above analysis, a cloud services provider that provides Infrastructure as a Service using a private or community deployment model is the best fit for FSFN. Migrating to an IaaS requires the lowest effort for development, migration, testing and training for transferring FSFN to a specific service.

# D. Cost Analysis

This section presents a cost analysis of the options. The options presented are for keeping FSFN with the AST and hosting FSFN in a cloud service that is Infrastructure as a Service (IaaS). There is additional cost analysis for a cloud service provider supplying both a mainframe and middle tier servers for FSFN, and migrating FSFN off the mainframe and onto middle tier servers at a cloud service provider. The cost analysis includes the following:

- The cost analysis for keeping FSFN with the AST includes the current Fiscal Year 2015/2016 as a baseline for the AST charges to DCF specific to FSFN. There are expected cost adjustments for the AST starting in Fiscal Year 2016/2017 to account for a new mainframe lease, which includes additional capacity for FSFN and the FLORIDA system. There are expected cost adjustments starting in Fiscal Year 2017/2018 to include increased costs for new hardware for FSFN related to a hardware refresh and updating the application to operate on the most current versions of software platforms.
- The cost analysis for migrating FSFN to a cloud service provider with a hosted mainframe and middle tier servers, is the second analysis included. The analysis starts with Fiscal Year 2016/2017 with the expectation of procuring cloud services to start July 1, 2016. The cost analysis includes the costs for cloud services, application support, disaster recovery, migration and a transition for the AST to maintain FSFN while migrating to the cloud.
- The cost analysis for migrating FSFN to a cloud service provider, with migration of FSFN off the mainframe and onto middle tier servers only. The analysis starts with Fiscal Year 2016/2017 with the expectation of procuring cloud services to start July 1, 2016. The cost analysis includes the costs of moving FSFN off the mainframe, cloud services, application support, disaster recovery, migration and a transition for the AST to maintain FSFN while migrating to the cloud.

## 1. Summary of Cost Benefit Analysis

An annual cost is used to analyze the cost benefits for each of the hosting options. To perform a like comparison across the three options, three categories of costs are used. The categories are Hosting Costs, Staffing Costs and Disaster Recovery. These three categories constitute the majority of the annual costs for hosting FSFN, as well as benefits related to these categories.

### *Hosting Costs*

The costs of hosting and services are used to compare providers. This excludes direct costs for staffing and disaster recovery, which are covered in a separate section below.

The AST hosting and services cost is an average price of $2,596,747.30 in Fiscal Year 2015/2016. The cloud service provider costs for the cloud option that includes both mainframe and middle tier averages $4,048,637.98 per year. The costs for the cloud option that includes only middle tier servers averages $1,558,648.35 per year.

Hosting at either of the two cloud service providers has some initial benefits. These include:

- FSFN is hosted in a Tier 3 Data Center
- Enforceable SLAs for availability of infrastructure
- Enforceable SLAs for addressing issues with LPARs and Virtual Machines
- Replacement of aging equipment is built into the hosting cost
- Ability to quickly scale an LPAR or Virtual Machine for additional capacity based on need
- Billing for utilization rather than capacity

The option requiring FSFN to operate only on middle tier servers has three potential risks, which are:

- Requires recoding and testing of critical COBOL batch jobs and JCL programs to Java in a short period of time

- Potential schedule risks due to the need to regression test and user acceptance test code changes related to migration off of the mainframe
- The mainframe components have a reliable history of performance and availability

**Finding**

Factoring in the risk and benefits of the hosting providers, the cloud service that requires FSFN to operate only on middle tier servers is the better option for hosting.

### *Staff Costs*

To compare support staff, staffing cost above those included with the hosting costs are used. This excludes staffing that is bundled with the costs of hosting and hosting services.

The AST cost for staffing and contractors averages $704,563.36 in Fiscal Year 2015/2016. For both of the cloud hosting options, there is an average annual cost of $2,708,333.33 to provide a dedicated team to support FSFN, beyond staff that are provided by the cloud service provider.

The benefits of having a dedicated staff to support FSFN in the cloud are:

- Enforceable SLAs for availability of application components such as Reporting, Batch, Interfaces and the FSFN Application
- Enforceable SLAs for the performance of application components
- Staff is 100% dedicated to supporting FSFN
- Staff would also perform tasks related to disaster recovery (Plan, Test, Execute)

**Finding**

The staff costs related to the cloud hosting options provides DCF with dedicated staff for the support of the FSFN application components and enforceable SLAs. This translates into an intangible benefit to the users of FSFN by improving system reliability and availability.

### *Disaster Recovery Costs*

To compare disaster recovery options, costs provided by each of the hosting options specifically for disaster recovery are used.

The AST cost for disaster recovery is $311,508.73 in Fiscal Year 2015/2016. For the cloud hosting option which includes both mainframe and middle tier, the average annual cost for disaster recovery is $1,514,122.61. For the cloud hosting option which includes only middle tier, the average annual cost for disaster recovery is $505,055.81.

Disaster Recovery for both of the Cloud hosting options for FSFN have the following benefits:

- Backups of systems and data are stored at the recovery site
- System and data are synchronized every 15 minutes
- Hardware is available within 24 hours of declaration of a disaster
- Disaster Recovery can be performed remotely, instead of traveling to a recovery site
- Ability to recover FSFN within 36 hours

The primary differences between Disaster Recovery for the two IaaS options is the cost of the mainframe and dedicated mainframe backups. These two items account for almost two thirds of the disaster recovery cost for the hosting option with both mainframe and middle tier.

**Finding**

The costs of Disaster Recovery supports choosing the cloud hosting option that requires FSFN to operate on middle tier servers only.

## 2. FSFN System Hosted at the AST

This analysis includes a baseline cost for FSFN hosted at the AST in Fiscal Year 2015/2016. There is an expected increase for the cost of hosting FSFN at the AST in Fiscal Year 2016/2017 due to a new mainframe lease. There is also an expected increase for the cost of a hardware refresh for all middle tier servers across all environments for FSFN in Fiscal Year 2017/2018.

| | FY 15/16 | Comments |
|---|---|---|
| **AST - Staffing Cost** | $ 696,467.36 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| **AST - Hardware Lease or Maintenance Cost** | $ 485,689.91 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| **AST - Software Lease or Maintenance Cost** | $ 1,241,176.74 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| **AST - Disaster Recovery** | $ 311,508.73 | AST Disaster Recovery includes Backups, Leasing Equipment at Sungard, and a Disaster Recovery Test<br>Expected recovery of FSFN in 7 days |
| **AST - Open Systems** | $ 1,525.00 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| **AST - Windows** | $ 1,181.00 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| **AST - Database** | $ 27.00 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| **AST - Contractor - LBR Network Installation** | $ 2,501.00 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| **AST - Contractor - LBR Implementation** | $ 5,595.00 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| **AST - Backup & Recovery** | $ 1,311.00 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| **AST - Network Bandwidth** | $ 5,287.48 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| **AST - Network Support** | $ 293.82 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |

| | FY 15/16 | Comments |
|---|---|---|
| **AST - Mainframe Support** | $ 2,461.00 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| **AST - Storage** | $ 276.00 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| **AST - Building Cost** | $ 5,633.00 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| **AST - Other Cost** | $ 8,700.00 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| **AST - Data Center Operations Cost** | $ 864.00 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| **AST - Equipment Depreciation** | $ 198,235.35 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| **AST - Indirect Costs** | $ 644,086.00 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| **Total** | **$ 3,612,819.39** | |

**AST Costs for Hosting FSFN from Fiscal Year 2015/2016 through Fiscal Year 2020/2021**

## 3. Infrastructure as a Service Costs

For Infrastructure as a Service (IaaS), it is assumed that the cloud computing service provider will only provide Hardware, Operating Systems, Network and associated support personnel to manage the environment per the scope of services from the cloud service provider. All software that needs to be installed beyond the Operating System will be purchased new or provided by the cloud service provider.

The cost analysis for the Infrastructure as a Service options will begin with Fiscal Year 2016/2017 and continue through Fiscal Year 2020/2021. The reason for selecting Fiscal Year 2016/2017 as the start is because it aligns with the budget year by which FSFN is expected to transition to the cloud (June 30, 2017).

### *Mainframe and Middle Tier Infrastructure as a Service*

For this option of Infrastructure as a Service (IaaS), it is assumed that FSFN will continue to run on a hybrid solution, which includes both mainframe and mid-Tier Servers. As part of the cloud computing services, a mainframe and multiple mid-tier servers will be provided that are equal to or more current than those hosted at the AST.

#### Cloud Service Provider Costs – For Mainframe and Middle Tier

The following are costs related to the hosting of FSFN at a cloud service provider. This includes:

- Tier 3 Data Center
- Dev, Test, Acceptance and Production Environments for both mainframe and middle tier
- Additional Software needed to run FSFN at the cloud service provider
- Storage, Backups, Local Area Network
- Support and Services for the Virtual Machines and LPARs
- Support and Services for Local Area Network, Storage, and Backups
- Support and Services for the Operating System
- Mainframe DB2 Physical DBA
- Regular hardware refresh
- Security Patching and Updates

| | FY 16/17 | FY 2017/2018 | FY 18/19 | FY 19/20 | FY 20/21 | Total | Comments |
|---|---|---|---|---|---|---|---|
| **Cloud Service Provider - Middle Tier Hardware** | $ 1,146,702.43 | $ 1,038,574.71 | $ 986,646.98 | $ 1,000,009.59 | $ 1,013,695.47 | $5,185,629.18 | Includes Hardware, Virtual Machines, Operating Systems, Storage, Local Area Network, Backups, Availability Service Levels, Outage Service Levels, Hardware Upgrades, Operating System Patching, Hardware Patching |
| **Cloud Service Provider - Mainframe Hardware, Software, Services** | $ 1,800,000.00 | $ 2,980,000.00 | $ 2,980,000.00 | $ 2,980,000.00 | $ 2,980,000.00 | $13,720,000.00 | Includes Hardware, LPARs, Operating Systems, Storage, Local Area Network, Backups, Availability Service Levels, Outage Service Levels, Hardware Upgrades, Operating System Patching, Hardware Patching<br>Includes zOS Standard Stack, DB2 Database, COBOL |
| **Cloud Service Provider - Middle Tier Software** | $ 903,702.00 | $ 189,777.42 | $ 199,266.29 | $ 209,229.61 | $ 219,691.09 | $1,721,666.41 | Includes Middle Tier Database and Application Servers |
| **Total** | **$ 3,850,404.43** | **$ 4,208,352.13** | **$ 4,165,913.27** | **$ 4,189,239.20** | **$ 4,213,386.56** | **$ 20,627,295.59** | |

**Cloud Service Provider Costs for Mainframe and Middle Tier Fiscal Year 2016/2017 through Fiscal Year 2020/2021**

### Disaster Recovery – For Mainframe and Middle Tier

The following are costs related to the disaster recovery option selected for a cloud service provider. This includes:

- Only production FSFN Application middle tier servers and mainframe are included
- Federated mainframe in a Disaster Recovery Site
- Mainframe hardware availability within 24 hours after disaster declaration
- Mainframe Backup equipment located at recovery site
- Replication scheduled by DCF
- Mainframe backups as a managed service
- DCF must restore mainframe from backups for recovery
- Active – Passive disaster recovery site for middle tier servers
- Middle tier site available within 4 hours after disaster declaration
- Middle tier data synchronized between sites every 15 minutes
- DCF must confirm recovery of middle tier servers
- Expected recovery time in 36 hours or less

| | FY 16/17 | FY 17/18 | FY 18/19 | FY 19/20 | FY 20/21 | Total | Comments |
|---|---|---|---|---|---|---|---|
| **Disaster Recovery** | $ 849,232.93 | $ 1,676,474.50 | $ 1,638,604.71 | $ 1,628,454.39 | $ 1,640,048.23 | $ 7,432,814.76 | Includes Federated Mainframe that is available within 24 hours<br>Includes Active - Passive Environments that are available within 4 hours<br>Includes Data Synchronization every 15 Minutes<br>Expected recovery in under 36 hours |
| **Total** | **$ 849,232.93** | **$ 1,676,474.50** | **$ 1,638,604.71** | **$ 1,628,454.39** | **$ 1,640,048.23** | **$ 7,432,814.76** | |

**Disaster Recovery Costs for Middle Tier and Mainframe for Fiscal Year 2016/2017 through Fiscal Year 2020/2021**

### Prerequisite Code Changes to FSFN – For Middle Tier and Mainframe

FSFN has a prerequisite for migrating to a cloud service provider that supplies mainframe and middle tier. The prerequisite is to modify code so that FSFN can run on software platforms that are at supported levels. This is a one-time cost in Fiscal Year 2016/2017.

| | FY 16/17 | FY 17/18 | FY 18/19 | FY 19/20 | FY 20/21 | Total | Comments |
|---|---|---|---|---|---|---|---|
| **Migration - Cloud Prerequisite Supported Platforms (Services)** | $ 2,851,200.00 | $ - | $ - | $ - | $ - | $ 2,851,200.00 | Includes the effort cost for recoding FSFN to operate on software platforms that are at supported levels. This represents the additional staff cost to reduce the overall effort from 3 years to 18 months, to meet the June 30, 2017 cloud deadline. |
| **Total** | **$ 2,851,200.00** | **$ -** | **$ -** | **$ -** | **$ -** | **$ 2,851,200.00** | |

**DCF Costs for Recoding Mainframe Components to Middle Tier for Fiscal Year 2016/2017 through Fiscal Year 2020/2021**

### Recurring Annual Costs for Cloud Hosting – For Mainframe and Middle Tier

The following are recurring annual costs for hosting FSFN in the cloud. This includes:

- Additional staff needed for the migration of FSFN to the cloud
- Additional dedicated staff needed to support FSFN after migration to the cloud, including:
  - Cloud Project Management
  - Technical Architecture Lead
  - Logical Database Administrators
  - Application Server Administrators
  - Report Server Administrators
  - Batch Server Administrators
  - Application Monitoring and Administration
- AST Indirect Costs (Fiscal Year 2016/2017 is included in AST Migration and Transition Costs in the Table on the Next Page)

| Hybrid Hosting Option | FY 16/17 | FY 17/18 | FY 18/19 | FY 19/20 | FY 20/21 | Total | Comments |
|---|---|---|---|---|---|---|---|
| **Recurring - Application Support Services** | $ 2,000,000.00 | $ 2,750,000.00 | $ 3,000,000.00 | $ 3,000,000.00 | $ 2,750,000.00 | $ 13,500,000.00 | Includes Cloud Project Management, Technical Architecture Lead, Logical Database Administrators, Application Server Administrators, Report Server Administrators, Batch Server Administrators, and Application Operational Support Staff |
| **Recurring - AST indirect costs** | $ - | $ 644,086.00 | $ 644,086.00 | $ 644,086.00 | $ 644,086.00 | $ 2,576,344.00 | Represents AST Indirect Cost that is planned to be assessed for 5 years |
| **Network Connection to Cloud Provider** | $ 351,120.00 | $ 152,120.00 | $ 152,120.00 | $ 152,120.00 | $ 152,120.00 | $ 959,600.00 | Represents DCF cost to provide connection to Cloud Service Provider |
| **Recurring - Application Support Services** | $2,351,120.00 | $3,546,206.00 | $3,796,206.00 | $3,796,206.00 | $3,546,206.00 | $17,035,944.00 | |

**Recurring Annual Costs for Middle Tier and Mainframe for Fiscal Year 2016/2017 through Fiscal Year 2020/2021**

### AST Costs for Migration and Transition – For Mainframe and Middle Tier

The table on the next page shows the AST costs related to migrating and transitioning FSFN to the cloud. This includes:

- AST Professional Services for Database and File Transfer Support for Migration
- AST Costs that continue for Fiscal Year 2016/2017 while FSFN runs at the AST during migration of the system to the cloud

| | FY 15/16 | Comments |
|---|---|---|
| Migration - AST Professional Services | $ 98,400.00 | Include AST Professional Services to assist with the migration of FSFN to the cloud |
| AST - Staffing Cost | $ 696,467.36 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| AST - Hardware Lease or Maintenance Cost | $ 485,689.91 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| AST - Software Lease or Maintenance Cost | $ 1,241,176.74 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| AST - Disaster Recovery | $ 311,508.73 | AST Disaster Recovery includes Backups, Leasing Equipment at Sungard, and a Disaster Recovery Test<br>Expected recovery of FSFN in 7 days |
| AST - Open Systems | $ 1,525.00 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| AST - Windows | $ 1,181.00 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| AST - Database | $ 27.00 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| AST - Contractor - LBR Network Installation | $ 2,501.00 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| AST - Contractor - LBR Implementation | $ 5,595.00 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| AST - Backup & Recovery | $ 1,311.00 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| AST - Network Bandwidth | $ 5,287.48 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| AST - Network Support | $ 293.82 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |

| | FY 15/16 | Comments |
|---|---|---|
| AST - Mainframe Support | $ 2,461.00 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| AST - Storage | $ 276.00 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| AST - Building Cost | $ 5,633.00 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| AST - Other Cost | $ 8,700.00 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| AST - Data Center Operations Cost | $ 864.00 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| AST - Equipment Depreciation | $ 198,235.35 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| AST - Indirect Costs | $ 644,086.00 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| **Sub Total** | **$ 3,711,219.00** | |

**AST Costs for Migration and Transition for Middle Tier and Mainframe for Fiscal Year 2016/2017**

### *Middle Tier Only Infrastructure as a Service*

For this option of Infrastructure as a Service (IaaS), it is assumed that FSFN components operating on the mainframe will be recoded to operate on a middle tier server. This cost will include the cost of recoding the mainframe components and the costs related to only middle tier servers at a cloud service provider.

#### Cloud Service Provider Costs – For Middle Tier

The following are costs related to hosting FSFN at a cloud service provider. This includes:

- Tier 3 Data Center
- Dev, Test, Acceptance and Production Environments for middle tier
- Additional Software needed to run FSFN at the Cloud service provider
- Storage, Backups, Local Area Network
- Support and Services for the Virtual Machines
- Support and Services for Local Area Network, Storage, and Backups
- Support and Services for the Operating System
- Regular hardware refresh
- Security Patching and Updates

| | FY 16/17 | FY 17/18 | FY 18/19 | FY 19/20 | FY 20/21 | Total | Comments |
|---|---|---|---|---|---|---|---|
| **Cloud Service Provider - Middle Tier Hardware** | $ 1,475,186.92 | $ 1,350,634.66 | $ 1,283,104.55 | $ 1,299,955.34 | $ 1,317,216.71 | $ 6,726,098.18 | Includes Hardware, Virtual Machines, Operating Systems, Storage, Local Area Network, Backups, Availability Service Levels, Outage Service Levels, Hardware Upgrades, Operating System Patching, Hardware Patching |
| **Cloud Service Provider - Middle Tier Software** | $ 903,702.00 | $ 189,777.42 | $ 199,266.29 | $ 209,229.61 | $ 219,691.09 | $ 1,721,666.41 | Includes Middle Tier Database and Application Servers |
| **Total** | **$ 2,378,888.92** | **$ 1,540,412.08** | **$ 1,482,370.84** | **$ 1,509,184.95** | **$ 1,536,907.80** | **$ 8,447,764.59** | |

**Cloud Service Provider Costs for Middle Tier Only for Fiscal Year 2016/2017 through Fiscal Year 2020/2021**

### Disaster Recovery – For Middle Tier

The following are costs related to the disaster recovery option selected for the cloud service provider. This includes:

- Active – Passive disaster recovery site for middle tier servers
- Middle tier site available within 4 hours after disaster declaration
- Middle tier data synchronized between sites every 15 minutes
- DCF must confirm recovery of middle tier servers
- Expected recovery time in 24 hours or less

| | FY 16/17 | FY 17/18 | FY 18/19 | FY 19/20 | FY 20/21 | Total | Comments |
|---|---|---|---|---|---|---|---|
| **Disaster Recovery** | $ 593,206.21 | $ 553,519.45 | $ 525,843.73 | $ 535,310.41 | $ 544,998.40 | $ 2,752,878.20 | Includes Active - Passive Environments that are available within 4 hours<br>Includes Data Synchronization every 15 Minutes<br>Expected recovery in under 24 hours |
| **Mid-Tier Hosting Option** | **$ 593,206.21** | **$ 553,519.45** | **$ 525,843.73** | **$ 535,310.41** | **$ 544,998.40** | **$ 2,752,878.20** | |

**Disaster Recovery Costs for Middle Tier only for Fiscal Year 2016/2017 through Fiscal Year 2020/2021**

### Recurring Annual Costs for Cloud Hosting – For Middle Tier

The following are recurring annual costs related hosting FSFN in the Cloud. This includes:

- Software licenses for reporting and batch servers
- Additional staff needed for the migration of FSFN to the Cloud
- Additional dedicated staff needed to support FSFN after migration to the Cloud, including:
  - Cloud Project Management
  - Technical Architecture Lead
  - Logical Database Administrators
  - Application Server Administrators
  - Report Server Administrators

  - Batch Server Administrators
  - Application Monitoring and Administration
- AST Indirect Costs (Fiscal Year 2016/2017 is included in AST Migration and Transition Costs in the next table)

| Mid-Tier Hosting Option | FY 16/17 | FY 17/18 | FY 18/19 | FY 19/20 | FY 20/21 | Total | Comments |
|---|---|---|---|---|---|---|---|
| **Recurring - Application Support Services** | $ 2,000,000.00 | $ 2,750,000.00 | $ 3,000,000.00 | $ 3,000,000.00 | $ 2,750,000.00 | $ 13,500,000.00 | Includes Cloud Project Management, Technical Architecture Lead, Logical Database Administrators, Application Server Administrators, Report Server Administrators, Batch Server Administrators, and Application Operational Support Staff |
| **Recurring - AST indirect costs** | $ - | $ 644,086.00 | $ 644,086.00 | $ 644,086.00 | $ 644,086.00 | $ 2,576,344.00 | Represents AST Indirect Cost that is planned to be assessed for 5 years |
| **Network Connection to Cloud Provider** | $ 351,120.00 | $ 152,120.00 | $ 152,120.00 | $ 152,120.00 | $ 152,120.00 | $ 959,600.00 | Represents DCF cost to provide connection to Cloud Service Provider |
| **Recurring - Application Support Services** | $2,351,120.00 | $3,546,206.00 | $3,796,206.00 | $3,796,206.00 | $3,546,206.00 | $17,035,944.00 | |

**Recurring Annual Costs for Middle Tier only for Fiscal Year 2016/2017 through Fiscal Year 2020/2021**

### Prerequisite Code Changes for FSFN– For Middle Tier

FSFN has two prerequisites for migrating to a cloud service provider that only supplies middle tier. The first prerequisite is to recode all COBOL and JCL mainframe code to Java to run on middle tier. The second is to modify code so that FSFN can run on software platforms that are at supported levels. This includes:

- Staff costs for recoding and testing COBOL batch jobs to Java
- Staff costs for recoding and testing JCL scripts to Java
- Modifying FSFN code to run on software platforms that are at supported levels

| | FY 16/17 | FY 17/18 | FY 18/19 | FY 19/20 | FY 20/21 | Total | Comments |
|---|---|---|---|---|---|---|---|
| Migration - Replatform Mainframe to Middle Tier | $ 2,043,200.00 | $ - | $ - | $ - | $ - | $ 2,043,200.00 | Includes the conversion of COBOL Batch Jobs and JCL Programs to Java |
| Migration - Cloud Prerequisite Supported Platforms | $ 2,851,200.00 | $ - | $ - | $ - | $ - | $ 2,851,200.00 | Includes the effort cost for recoding FSFN to operate on software platforms that are at supported levels. This represents the additional staff cost to reduce the overall effort from 3 years to 18 months, to meet the June 30, 2017 cloud deadline. |
| **Total** | **$ 4,894,400.00** | **$ -** | **$ -** | **$ -** | **$ -** | **$ 4,894,400.00** | |

**AST Costs for Recoding Mainframe Components to Middle Tier for Fiscal Year 2016/2017 through Fiscal Year 2020/2021**

### AST Costs for Migration and Transition – For Middle Tier

The following are AST costs related to migrating and transitioning FSFN to the cloud. This includes:

- AST Professional Services for Database and File Transfer Support for Migration
- AST Costs that continue for Fiscal Year 2016/2017 while FSFN runs at the AST during migration to the cloud

| | FY 16/17 | FY 17/18 | FY 18/19 | FY 19/20 | FY 20/21 | Total | Comments |
|---|---|---|---|---|---|---|---|
| Migration - AST Professional Services | $ 98,400.00 | | | | | $ 98,400.00 | Include AST Professional Services to assist with the migration of FSFN to the cloud |
| AST - Staffing Cost* | $ 96,467.36 | | | | | $ 696,467.36 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| AST - Hardware Lease or Maintenance Cost* | $ 485,689.91 | | | | | $ 485,689.91 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| AST - Software Lease or Maintenance Cost* | $1,241,176.74 | | | | | $1,241,176.74 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| AST - Disaster Recovery* | $ 311,508.73 | | | | | $ 311,508.73 | AST Disaster Recovery includes Backups, Leasing Equipment at Sungard, and a Disaster Recovery Test Expected recovery of FSFN in 7 days |

| | FY 16/17 | FY 17/18 | FY 18/19 | FY 19/20 | FY 20/21 | Total | Comments |
|---|---|---|---|---|---|---|---|
| AST - Open Systems* | $ 1,525.00 | | | | | $ 1,525.00 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| AST - Windows* | $ 1,181.00 | | | | | $ 1,181.00 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| AST - Database* | $ 27.00 | | | | | $ 27.00 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| AST - Contractor - LBR Network Installation* | $ 2,501.00 | | | | | $ 2,501.00 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| AST - Contractor - LBR Implementation* | $ 5,595.00 | | | | | $ 5,595.00 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| AST - Backup & Recovery* | $ 1,311.00 | | | | | $ 1,311.00 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| AST - Network Bandwidth* | $ 5,287.48 | | | | | $ 5,287.48 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| AST - Network Support* | $ 293.82 | | | | | $ 293.82 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |

| | FY 16/17 | FY 17/18 | FY 18/19 | FY 19/20 | FY 20/21 | Total | Comments |
|---|---|---|---|---|---|---|---|
| AST - Mainframe Support* | $ 2,461.00 | | | | | $ 2,461.00 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| AST - Storage* | $ 276.00 | | | | | $ 276.00 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| AST - Building Cost* | $ 5,633.00 | | | | | $ 5,633.00 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| AST - Other Cost* | $ 8,700.00 | | | | | $ 8,700.00 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| AST - Data Center Operations Cost* | $ 864.00 | | | | | $ 864.00 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| AST - Equipment Depreciation* | $ 98,235.35 | | | | | $ 198,235.35 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| AST - Indirect Costs* | $ 644,086.00 | | | | | $ 644,086.00 | Reflects AST Cost that continues while FSFN is migrated to the Cloud |
| **Sub Total** | **$ 3,711,219** | **$ -** | **$ -** | **$ -** | **$ -** | **$3,711,219.39** | |

** Denotes Fiscal Year 2015/2016 were used as a forecast of Fiscal Year 2016/2017 costs*

**AST Costs for Migration and Transition for Middle Tier for Fiscal Year 2016/2017 through Fiscal Year 2020/2021**

# E. Qualitative and Quantitative Benefits

The proviso language in the 2015/2016 Budget asks for the qualitative and quantitative analysis of the benefits of migrating FSFN to a cloud service provider. This appendix provides details, results and findings of our research.

## Findings

The following sections contain a description of the benefits of migrating FSFN to a cloud service provider.

## Cloud Hosting

The following benefits are derived from the use of cloud hosting for the FSFN Infrastructure.

- Infrastructure as a Service is a Utility Service. This means that the service model uses a Pay Per Use or Pay Per Go subscription model.
- Infrastructure as a Service is also a Metered Service. This means that usage is metered and priced on the basis of units consumed. This allows customers to pay for what you use and when you use it.
- There are no capital investments for system components hosted in the cloud. Using the cloud service provider's servers, storage and network hardware, there is no need to invest in computing infrastructure, maintenance or space to store equipment.
- Cloud hosting allows for an increased speed in decision making and acting on decisions by being agile and dynamic in providing technology.
- Hosting costs are predictable, avoiding spikes in expenditures for periodically replacing aging infrastructure. This allows for more reliable long term financial planning.

## Physical Data Center

For the cloud service provider selected for this plan, the physical data center offers several benefits to FSFN. These benefits are as follows:

- Tier 3 Data Center
    - Multiple independent distribution paths serving the IT equipment
    - All IT equipment must be dual powered and fully compatible with the topology of a site's architecture
    - Concurrently maintainable site infrastructure with expected availability of 99.982%
- SSAE16 certified Data Center, Rack Space, Power and Cooling
- Increase in infrastructure reliability and performance
- Redundant Paths to Public Utility Provider
- Dual Power Feeds to all Air Conditioners
- Redundant Air Conditioning
- UPS Battery Power with N+1 Redundancy
- EPS Generator Power System with N+1 Redundancy
- On Site Diesel Storage for 48 Hours Full Load
- Power Distribution Units Loaded to 45% Capacity
- Redundant Critical Alarm Systems for Monitoring Environmental Conditions
- Concurrent maintenance capability down to the PDU level
- Preventative maintenance schedule for all critical systems
- Fire suppression and smoke detection
- Monthly testing of backup power generator systems
- Yearly "drop dead" test of all backup systems

Note that the Southwood Resource Center is a Tier 3 Data Center and offers many of the physical data center benefits that are associated with the cloud service provider.

### Hardware

When considering the hardware needed to support FSFN, the hardware at the cloud service provider offers several benefits over the current hosting of FSFN at the Northwood Resource Center.

- Reduces the need for capital expenditure for the upgrade of unique hardware, such as a mainframe
- Hardware upgrades are a predictable operational expenditure versus periodic capital expenditures
- All middle tier servers will be virtualized
- All middle tier servers will be scalable
- Mainframe system will be scalable
- Scaling up virtual machines and mainframe is upon request
- Supports hardware needed to run the FSFN Production Application Database off of the mainframe
- Provides options for storage performance based on the usage of the storage (For example High I/O vs Low I/O)
- Dual 155 Mbps shared private MPLS and managed site-to-site VPN
- Managed switches and routers. 10Gbps LAN
- 8Gbps FC SAN Storage
- Provides options for high end server technology for high transaction databases
- Technology refresh done by cloud service provider on fixed schedule at the cloud service provider's expense
- For the mainframe, the cost is based on usage and not allocation
- The use of current technology provides performance improvements

Note that the Southwood Resource Center is a Tier 3 Data Center and offers many of the physical data center benefits that are associated with the cloud service provider.

### Infrastructure Support

Infrastructure Support involves the tools and processes for providing management and monitoring of the technical infrastructure. The cloud service provider offers the following benefits over the Northwood Resource Center, as it relates to Infrastructure Support:

- Monitors the Status of each Virtual Machine
- Automatically Creates Event Tickets for Virtual Machine Issues
- Monitors Network for LAN where Virtual Machines are Located
- Response time for infrastructure and virtual machines is based on the Severity of the issue.
    - Severity 1 (complete outage) has a target resolution time 90% within 4 hours.
    - Severity 2 (key component outage or degradation) has a target resolution time 90% within 24 hours.
    - Severity 3 (component outage with work around) has a target response time of 7 calendar days.
    - Severity 4 (non-critical component outage with not impact to services) has a target response time of 30 calendar days.

### Support Personnel

Support Personnel refers to the staff that provide services related to the hosted system. This includes monitoring, backups, service requests and more. The benefits are as follows:

- High quality of service and support performance
- Higher ratio of infrastructure to resource, reducing overall cost

### High Availability

High Availability refers to the ability to keep the application functioning and accessible on a continuous basis. This includes Service Levels, Redundancy and Disaster Recovery. The benefits are as follows:

- Well Defined Response Service Levels Based on Severity of Virtual Machine or Network Outage
- Redundant Facility Features Including Power, Backups, Cooling and Monitoring
- Offers three tiers of availability ranging from 99.95% availability at the highest level to 99.5% at the lowest level

Note that the Southwood Resource Center is a Tier 3 Data Center and offers many of the physical data center benefits that are associated with the cloud service provider.

### Service Levels

Moving FSFN to the cloud would result in enforceable service levels for infrastructure performance and hardware break/fix.

- Enforceable service levels for the performance of the Cloud Infrastructure
- Enforceable service levels for managed services provided by the cloud service provider
- Enforceable service levels for application availability and performance
- Enforceable service levels for hardware break/fix

### Disaster Recovery

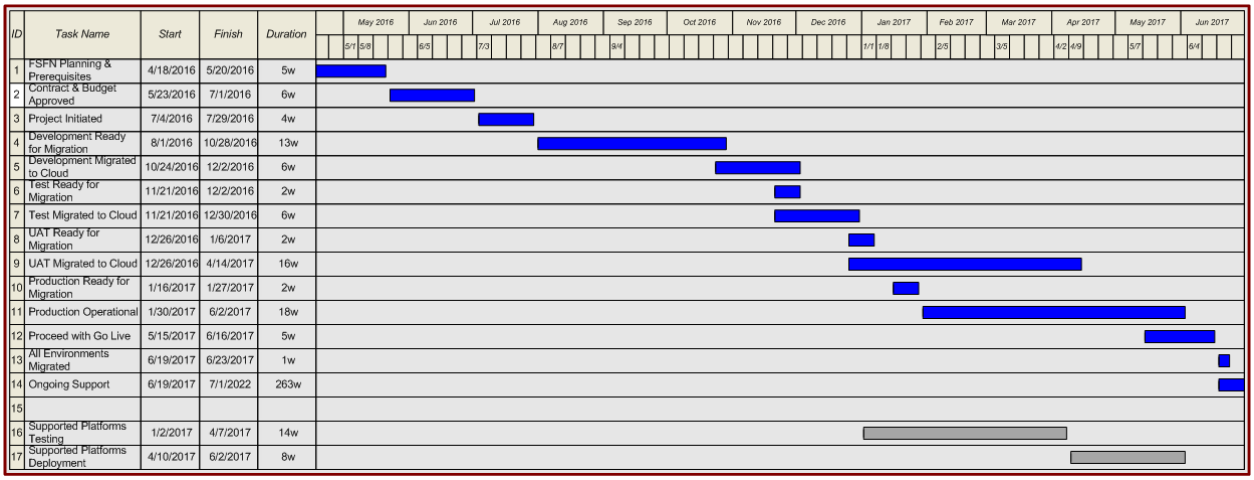
Disaster Recovery for the cloud service provider is improved. A recent test of the current disaster recovery solution allowed system recovery in 108 hours after the recovery site was turned over to the recovery team.

- Mainframe hardware is available 24 hours after an emergency is declared
- Middle tier hardware is available 4 hours after an emergency is declared
- Data is synchronized every 15 minutes between primary and disaster recovery site
- Recovery of FSFN can occur within 36 hours

# F. Implementation Plan

This final section of the report provides an Implementation Plan for Cloud Migration. The implementation plan includes the Work Breakdown Structure (WBS) for the tasks that must be completed for FSFN to reach a production ready state at the cloud services provider's facilities.

Within the plan, the tasks, responsible organization, task durations, sequence of the tasks and integrated schedule are defined. The estimated schedule is 62 weeks, commencing the week of April 16, 2016, and concluding prior to the June 30, 2017 deadline specified in the budget proviso language.



| ID | Task Name | Start | Finish | Duration |
|---|---|---|---|---|
| 1 | FSFN Planning & Prerequisites | 4/18/2016 | 5/20/2016 | 5w |
| 2 | Contract & Budget Approved | 5/23/2016 | 7/1/2016 | 6w |
| 3 | Project Initiated | 7/4/2016 | 7/29/2016 | 4w |
| 4 | Development Ready for Migration | 8/1/2016 | 10/28/2016 | 13w |
| 5 | Development Migrated to Cloud | 10/24/2016 | 12/2/2016 | 6w |
| 6 | Test Ready for Migration | 11/21/2016 | 12/2/2016 | 2w |
| 7 | Test Migrated to Cloud | 11/21/2016 | 12/30/2016 | 6w |
| 8 | UAT Ready for Migration | 12/26/2016 | 1/6/2017 | 2w |
| 9 | UAT Migrated to Cloud | 12/26/2016 | 4/14/2017 | 16w |
| 10 | Production Ready for Migration | 1/16/2017 | 1/27/2017 | 2w |
| 11 | Production Operational | 1/30/2017 | 6/2/2017 | 18w |
| 12 | Proceed with Go Live | 5/15/2017 | 6/16/2017 | 5w |
| 13 | All Environments Migrated | 6/19/2017 | 6/23/2017 | 1w |
| 14 | Ongoing Support | 6/19/2017 | 7/1/2022 | 263w |
| 15 | | | | |
| 16 | Supported Platforms Testing | 1/2/2017 | 4/7/2017 | 14w |
| 17 | Supported Platforms Deployment | 4/10/2017 | 6/2/2017 | 8w |



**High Level Implementation Plan**

It is important to note that prerequisite to migrating FSFN to a cloud service provider are version upgrades of the FSFN software platforms. The original plan was to perform that upgrade over a three-year period. However, the upgrades need to be completed prior to the migration to the cloud. In order to accommodate that requirement, the upgrade to supported platforms must be compressed to 18 months.

The Implementation Plan is key to managing the execution of the cloud migration and it leverages the established project management practices already in use by DCF. These include the current Governance, Deployment Procedures, Change Management and Risk Mitigation procedures.

## 1. Implementation Plans for Mainframe and Mid-Tier Options

In this section, there will be two plans presented. The two plans represent the timelines for migrating FSFN to a cloud service provider with a mainframe and without a mainframe. Both plans are similar in the steps taken to perform the migration, but there are subtle differences. This is why it is presented in two separate plans.

When creating a plan for migrating FSFN to a cloud service provider, there is focus on reducing the overall risk and increasing the likelihood of success for DCF and its users. The plan contains key milestones related to the migration of FSFN. These milestones represent checkpoints that need to be completed successfully before the next set of tasks can begin. At each of these checkpoints, DCF would participate in review of deliverables and other documentation to determine the readiness of the plan to move forward. For example, the development environment must be successfully migrated and the plan updated with lessons learned before work can begin on the test environment.

The plan starts by focusing on the migration of the development environments to the cloud first, followed by test environments, then the user acceptance environments and finally to the production environment. With each subsequent migration, lessons learned from the prior migration are integrated into the overall technical process. The goal is to have a detailed technical process that includes all lessons learned to minimize risks of issues occurring during migration to the production environment.

To support this iterative approach to process improvement, there should be a strong testing effort. The testing effort is based upon the framework currently employed at DCF. This testing framework includes creation of test scripts, smoke testing, component testing, acceptance testing, regression testing, performance testing and security testing. The framework will be used to validate each environment (development, test, user acceptance and production) after it has migrated to the cloud service provider.

Throughout the process there will be communications between the team performing the migration tasks, DCF IT Leadership and the business units. The execution of the plan will leverage the communication framework that already exists for technology projects at DCF. This includes frequent meetings with members of DCF IT to discuss status, review deliverables and identify risks and issues. In addition to these regular meetings, there will be a weekly stakeholder meeting between DCF Leadership, DCF IT and OCW to discuss program status, risks and issues.

The following sections represent the Work Breakdown Structure for the two Infrastructure as a Service Options. This includes the tasks that are planned to occur in migrating FSFN to a cloud service provider. The tasks will be arranged in the approximate order they need to occur and the tasks will have an approximate duration assigned to them.

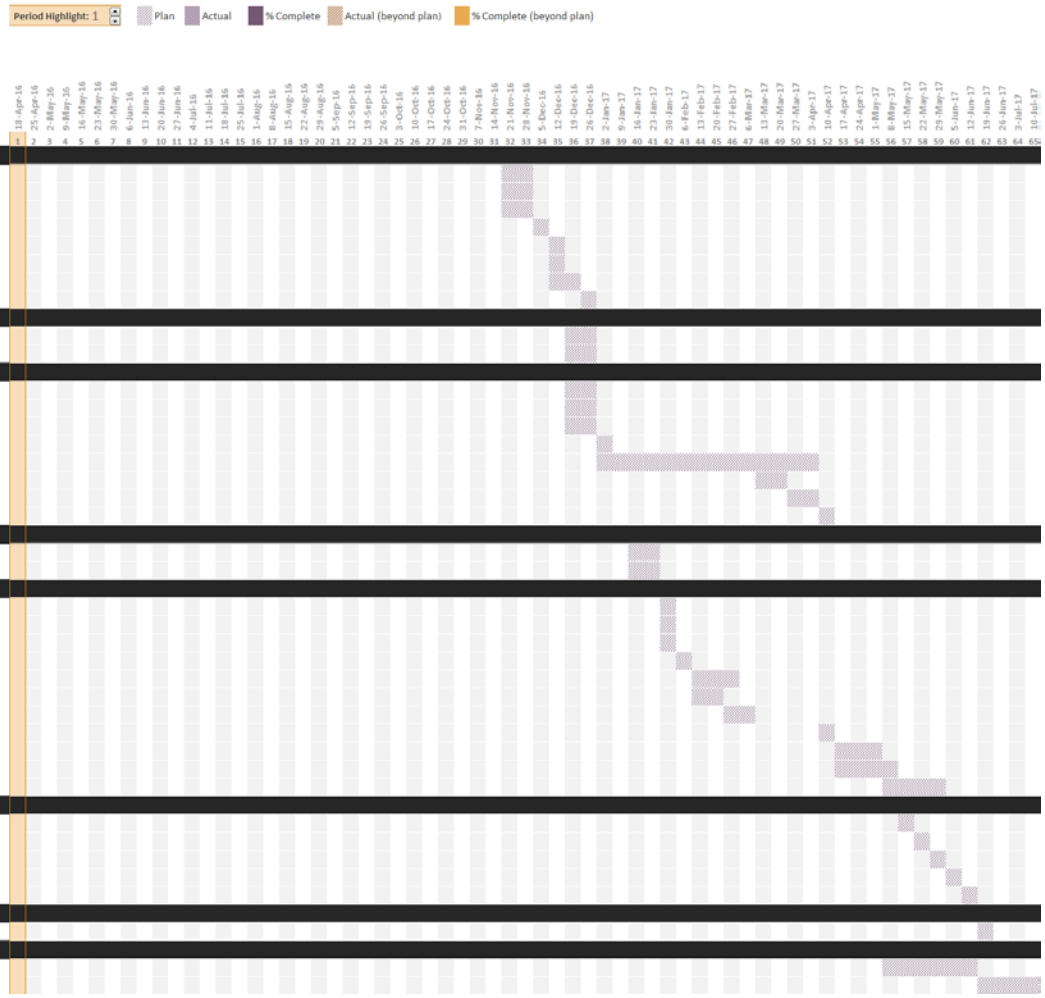
## 2. Infrastructure as a Service (Hybrid/Blended Hosting Option)

The following plan represents the steps needed to migrate FSFN to a cloud service provider using both mainframe and middle tier hardware that is equivalent to those provided in the existing system.

# IaaS Plan (with Mainframe)


| ACTIVITY | RESPONSIBLE PARTY(IES) | PLAN START (WEEK) | PLAN DURATION (IN WEEKS) | ACTUAL START (WEEK) | ACTUAL DURATION (IN WEEKS) | PERCENT COMPLETE |
|---|---|---|---|---|---|---|
| **Milestone: FSFN Upgrade to Supported Platforms** | | | | | | |
| Phase 1: Reporting Acceptance Testing | DCF | 38 | 8 | | | 0% |
| Phase 1: Reporting Production Deployment | DCF | 52 | 8 | | | 0% |
| Phase 2: ETL Acceptance Testing | DCF | 46 | 2 | | | 0% |
| Phase 2: ETL Production Deployment | DCF | 52 | 8 | | | 0% |
| Phase 3: Java Application Acceptance Testing | DCF | 48 | 4 | | | 0% |
| Phase 3: Java Application Production Deployment | DCF | 52 | 8 | | | 0% |
| Phase 4: Abuse Hotline and Portal | DCF | 1 | 20 | | | 0% |
| Supported Platforms Effort Completed | DCF | 60 | 1 | | | 0% |
| **Milestone: FSFN System Ready for Migration to Cloud** | | | | | | |
| Create Architecture Plan | DCF, CSP | 1 | 4 | | | 0% |
| Create Security Plan | DCF, CSP | 1 | 4 | | | 0% |
| Create Network Plan | DCF, CSP | 1 | 4 | | | 0% |
| Create Detailed Migration Plan | DCF, CSP | 1 | 4 | | | 0% |
| Create Disaster Recovery Plan | DCF, CSP | 1 | 4 | | | 0% |
| Create Test Plan | DCF | 1 | 4 | | | 0% |
| FedRAMP Security Assessment | DCF | 1 | 1 | | | 0% |
| FDLE Approval | DCF | 2 | 3 | | | 0% |
| ADP filed With ACF Bur of Children | DCF | 2 | 4 | | | 0% |
| DCF Approval of Plans | DCF | 5 | 1 | | | 0% |
| **Milestone: All Requisite Plans Created and Approved** | | | | | | |
| Draft SOW | DCF | 4 | 4 | | | 0% |
| Review and Discuss Hosting T&Cs | DCF | 5 | 4 | | | 0% |
| Update Hosting Quote | DCF, CSP | 9 | 2 | | | 0% |
| Finalize Contract | DCF | 10 | 2 | | | 0% |
| Obtain Budget Approval | DCF | 12 | 1 | | | 0% |
| **Milestone: Contract and Budget Approved** | | | | | | |
| Execute Contract | DCF | 12 | 2 | | | 0% |
| Project Kick Off | DCF, CSP | 14 | 1 | | | 0% |
| Purchase Necessary Software Licenses | DCF, CSP | 14 | 3 | | | 0% |
| Mainframe Build Out (LPARs, SW, Cfg) | CSP | 14 | 12 | | | 0% |
| Mid-Tier Build Out (HW/OS Only) | CSP | 20 | 8 | | | 0% |
| Install and Configure Monitoring Tools | CSP | 22 | 4 | | | 0% |
| Request MF to MT Network Connection | CSP | 20 | 8 | | | 0% |
| Request AST to CP Network Connection | CSP | 20 | 8 | | | 0% |
| Test Network Connectivity | CSP | 27 | 1 | | | 0% |
| Install/Configure DEV Mid-Tier Software | DCF | 28 | 2 | | | 0% |
| Develop Detailed Migration Checklist | DCF, CSP | 28 | 2 | | | 0% |
| **Milestone: Development Environment Ready for Migration** | | | | | | |
| Configure DEV LDAP Security | DCF, CSP | 28 | 2 | | | 0% |
| Configure DEV Mainframe Database | DCF, CSP | 28 | 2 | | | 0% |
| Configure DEV Mid-Tier Databases | DCF, CSP | 28 | 2 | | | 0% |
| Copy Selected DEV Environment to Cloud | DCF | 30 | 1 | | | 0% |
| Smoke Test DEV Environment in Cloud | DCF | 31 | 1 | | | 0% |
| Remediate Faults in DEV Environment | DCF, CSP | 32 | 1 | | | 0% |
| Copy All DEV Environments to Cloud | DCF | 33 | 1 | | | 0% |
| **Milestone: All Development Environments Migrated to Cloud** | | | | | | |
| Install/Configure TST Mid-Tier Software | DCF | 32 | 2 | | | 0% |
| Refine Detailed Migration Checklist | DCF | 32 | 2 | | | 0% |

# IaaS Plan (with Mainframe)




| ACTIVITY | RESPONSIBLE PARTY(IES) | PLAN START (WEEK) | PLAN DURATION (IN WEEKS) | ACTUAL START (WEEK) | ACTUAL DURATION (IN WEEKS) | PERCENT COMPLETE |
|---|---|---|---|---|---|---|
| **Milestone: Test Environment Ready for Migration** | | | | | | |
| Configure TST LDAP Security | DCF, CSP | 32 | 2 | | | 0% |
| Configure TST Mainframe Database | DCF, CSP | 32 | 2 | | | 0% |
| Configure TST Mid-Tier Databases | DCF, CSP | 32 | 2 | | | 0% |
| Copy Selected TST Environment to Cloud | DCF | 34 | 1 | | | 0% |
| Smoke Test TST Environment in Cloud | DCF | 35 | 1 | | | 0% |
| Integration Test for TST Environment in Cloud | DCF | 35 | 1 | | | |
| Remediate Faults in TST Environment | DCF, CSP | 35 | 2 | | | 0% |
| Copy All TST Environments to Cloud | DCF | 37 | 1 | | | 0% |
| **Milestone: All Test Environments Migrated to Cloud** | | | | | | |
| Install/Configure UAT Mid-Tier Software | DCF | 36 | 2 | | | 0% |
| Refine Detailed Migration Checklist | DCF | 36 | 2 | | | 0% |
| **Milestone: UAT Environment Ready for Migration** | | | | | | |
| Configure UAT LDAP Security | DCF, CSP | 36 | 2 | | | 0% |
| Configure UAT Mainframe Database | DCF, CSP | 36 | 2 | | | 0% |
| Configure UAT Mid-Tier Databases | DCF, CSP | 36 | 2 | | | 0% |
| Copy Selected UAT Environment to Cloud | DCF | 38 | 1 | | | 0% |
| Smoke Test UAT Environment in Cloud | DCF | 38 | 14 | | | 0% |
| Integration Test for UAT Environment in Cloud | DCF | 48 | 2 | | | 0% |
| Remediate Faults in UAT Environment | DCF, CSP | 50 | 2 | | | 0% |
| Copy All UAT Environments to Cloud | DCF | 52 | 1 | | | 0% |
| **Milestone: All UAT Environments Migrated to the Cloud** | | | | | | |
| Install/Configure PROD Mid-Tier Software | DCF | 40 | 2 | | | 0% |
| Refine Detailed Migration Checklist | DCF, CSP | 40 | 2 | | | 0% |
| **Milestone: Production Environment Ready for Migration** | | | | | | |
| Configure PROD LDAP Security | DCF, CSP | 42 | 1 | | | 0% |
| Configure PROD Mainframe Database | DCF, CSP | 42 | 1 | | | 0% |
| Configure PROD Mid-Tier Databases | DCF, CSP | 42 | 1 | | | 0% |
| Copy Preliminary PROD Environment to Cloud | DCF | 43 | 1 | | | 0% |
| Integration Test for PROD Environment in Cloud | DCF | 44 | 3 | | | 0% |
| Configure DR Site | CSP | 44 | 2 | | | 0% |
| Confirm DR Site | CSP | 46 | 2 | | | 0% |
| Copy Supported Platforms Code Stream to PROD in Cloud | DCF | 52 | 1 | | | 0% |
| Regression Test PROD Environment in Cloud | DCF | 53 | 3 | | | 0% |
| Remediate Faults in PROD Environment | DCF, CSP | 53 | 4 | | | 0% |
| User Acceptance Test PROD Environment in Cloud | DCF | 56 | 4 | | | 0% |
| **Milestone: Production Environment Confirmed Operational** | | | | | | |
| Create Go Live Checklist (Hour by Hour Plan) | DCF | 57 | 1 | | | 0% |
| Approve Go Live Check List | DCF | 58 | 1 | | | 0% |
| Migration Rehearsal #1 | DCF | 59 | 1 | | | 0% |
| Migration Rehearsal #2 | DCF | 60 | 1 | | | 0% |
| Go/No-Go Check Point | DCF | 61 | 1 | | | 0% |
| **Milestone: Confirmed Proceed With Go-Live** | | | | | | |
| Final Migration/Go Live | DCF | 62 | 1 | | | 0% |
| **Milestone: All Environments Migrated** | | | | | | |
| Cloud Environment Training | DCF, CSP | 56 | 6 | | | 0% |
| Ongoing Cloud Support | CSP | 62 | 263 | | | 0% |

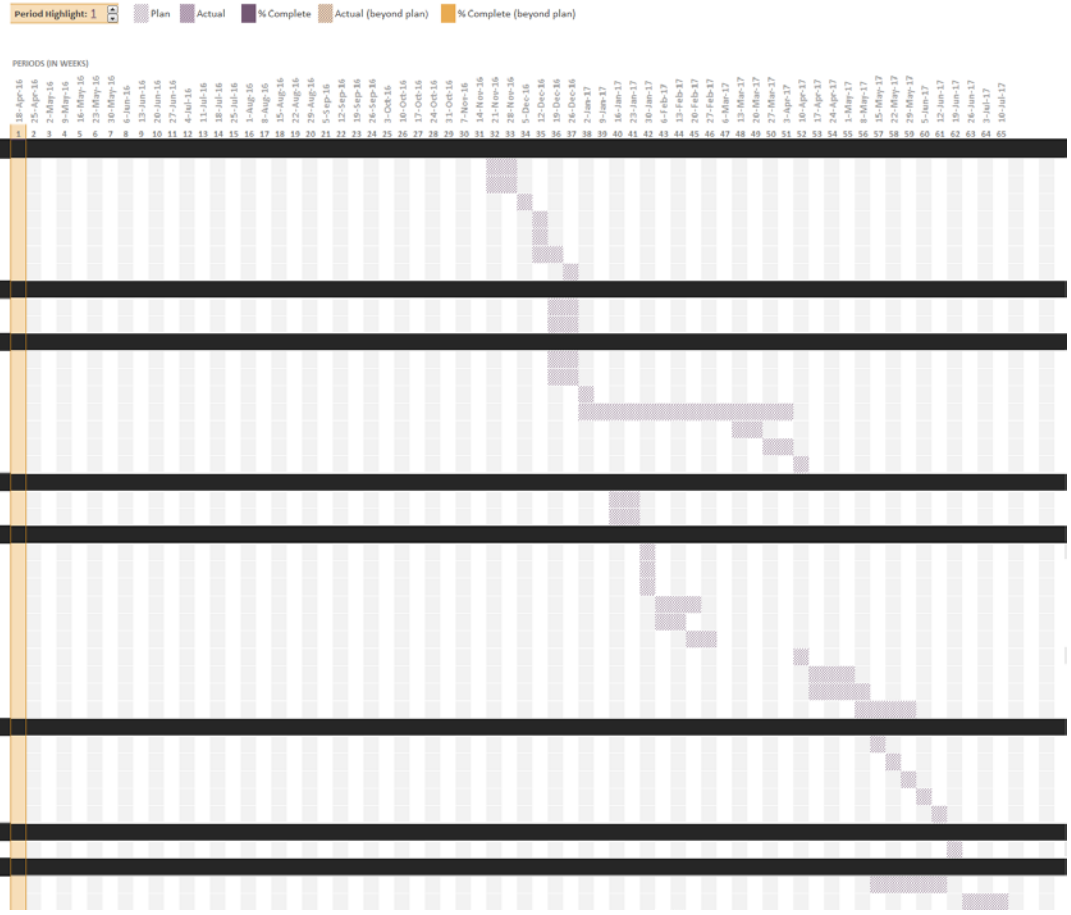
## 3. Infrastructure as a Service (Mid-Tier Hosting Option)

The following plan represents the steps needed to migrate FSFN to a cloud service provider using only middle tier hardware.

# IaaS Plan (without Mainframe)


| ACTIVITY | RESPONSIBLE PARTY(IES) | PLAN START (WEEK) | PLAN DURATION (IN WEEKS) | ACTUAL START (WEEK) | ACTUAL DURATION (IN WEEKS) | PERCENT COMPLETE |
|---|---|---|---|---|---|---|
| **Milestone: FSFN Upgrade to Supported Platforms** | | | | | | 0% |
| Phase 1: Reporting Acceptance Testing | DCF | 38 | 8 | | | 0% |
| Phase 1: Reporting Production Deployment | DCF | 52 | 8 | | | 0% |
| Phase 2: ETL Acceptance Testing | DCF | 46 | 2 | | | 0% |
| Phase 2: ETL Production Deployment | DCF | 52 | 8 | | | 0% |
| Phase 3: Java Application Acceptance Testing | DCF | 48 | 4 | | | 0% |
| Phase 3: Java Application Production Deployment | DCF | 52 | 8 | | | 0% |
| Phase 4: Abuse Hotline and Portal Testing and Deployment | DCF | 1 | 20 | | | 0% |
| Phase 5: Convert Cobol Batch Programs to Java Testing | DCF | 48 | 3 | | | 0% |
| Phase 5: Convert Cobol Batch Programs to Java Deployment | DCF | 52 | 8 | | | 0% |
| Supported Platforms Effort Completed | DCF | 60 | 1 | | | 0% |
| **Milestone: FSFN System Ready for Migration to Cloud** | | | | | | 0% |
| Create Architecture Plan | DCF, CSP | 1 | 4 | | | 0% |
| Create Security Plan | DCF, CSP | 1 | 4 | | | 0% |
| Create Network Plan | DCF, CSP | 1 | 4 | | | 0% |
| Create Detailed Migration Plan | DCF, CSP | 1 | 4 | | | 0% |
| Create Disaster Recovery Plan | DCF, CSP | 1 | 4 | | | 0% |
| Create Test Plan | DCF | 1 | 4 | | | 0% |
| Create MF to MT Project Plan | DCF | 1 | 4 | | | 0% |
| FedRAMP Security Assessment | DCF | 1 | 1 | | | 0% |
| FDLE Approval | DCF | 2 | 3 | | | 0% |
| ADP filed With ACF Bur of Children | DCF | 2 | 4 | | | 0% |
| DCF Approval of Plans | DCF | 5 | 1 | | | 0% |
| **Milestone: All Requisite Plans Created and Approved** | | | | | | 0% |
| Draft SOW | DCF | 4 | 4 | | | 0% |
| Review and Discuss Hosting T&Cs | DCF | 5 | 4 | | | 0% |
| Update Hosting Quote | DCF, CSP | 9 | 2 | | | 0% |
| Finalize Contract | DCF | 10 | 2 | | | 0% |
| Obtain Budget Approval | DCF | 12 | 1 | | | 0% |
| **Milestone: Contract and Budget Approved** | | | | | | 0% |
| Execute Contract | DCF | 12 | 2 | | | 0% |
| Project Kick Off | DCF, CSP | 14 | 2 | | | 0% |
| Modify FSFN System to Operate without Mainframe | DCF | 16 | 12 | | | 0% |
| Purchase Necessary Software Licenses | DCF, CSP | 17 | 3 | | | 0% |
| Mid-Tier Build Out (HW/OS Only) | CSP | 20 | 8 | | | 0% |
| Install and Configure Monitoring Tools | CSP | 24 | 4 | | | |
| Request AST to CP Network Connection | CSP | 20 | 8 | | | 0% |
| Test Network Connectivity | CSP | 27 | 1 | | | 0% |
| Install/Configure DEV Mid-Tier Software | DCF | 28 | 2 | | | 0% |
| Develop Detailed Migration Checklist | DCF, CSP | 28 | 2 | | | 0% |
| **Milestone: Development Environment Ready for Migration** | | | | | | 0% |
| Configure DEV LDAP Security | CSP, DCF | 28 | 2 | | | 0% |
| Configure DEV Mid-Tier Databases | CSP, DCF | 28 | 2 | | | 0% |
| Copy Selected DEV Environment to Cloud | CSP, DCF | 30 | 1 | | | 0% |
| Smoke Test DEV Environment in Cloud | DCF | 31 | 1 | | | 0% |
| Remediate Faults in DEV Environment | CSP, DCF | 32 | 1 | | | 0% |
| Copy All DEV Environments to Cloud | CSP, DCF | 33 | 1 | | | 0% |
| **Milestone: All Development Environments Migrated to Cloud** | | | | | | 0% |
| Install/Configure TST Mid-Tier Software | DCF | 32 | 2 | | | 0% |
| Refine Detailed Migration Checklist | DCF | 32 | 2 | | | 0% |

# IaaS Plan (without Mainframe)




| ACTIVITY | RESPONSIBLE PARTY(IES) | PLAN START (WEEK) | PLAN DURATION (IN WEEKS) | ACTUAL START (WEEK) | ACTUAL DURATION (IN WEEKS) | PERCENT COMPLETE |
|---|---|---|---|---|---|---|
| **Milestone: Test Environment Ready for Migration** | | | | | | 0% |
| Configure TST LDAP Security | CSP, DCF | 32 | 2 | | | 0% |
| Configure TST Mid-Tier Databases | CSP, DCF | 32 | 2 | | | 0% |
| Copy Selected TST Environment to Cloud | CSP, DCF | 34 | 1 | | | 0% |
| Smoke Test TST Environment in Cloud | DCF | 35 | 1 | | | 0% |
| Integration Test for TST Environment in Cloud | DCF | 35 | 1 | | | 0% |
| Remediate Faults in TST Environment | CSP, DCF | 35 | 2 | | | 0% |
| Copy All TST Environments to Cloud | CSP, DCF | 37 | 1 | | | 0% |
| **Milestone: All Test Environments Migrated to Cloud** | | | | | | 0% |
| Install/Configure UAT Mid-Tier Software | DCF | 36 | 2 | | | 0% |
| Refine Detailed Migration Checklist | DCF | 36 | 2 | | | 0% |
| **Milestone: UAT Environment Ready for Migration** | | | | | | 0% |
| Configure UAT LDAP Security | CSP, DCF | 36 | 2 | | | 0% |
| Configure UAT Mid-Tier Databases | CSP, DCF | 36 | 2 | | | 0% |
| Copy Selected UAT Environment to Cloud | CSP, DCF | 38 | 1 | | | 0% |
| Smoke Test UAT Environment in Cloud | DCF | 38 | 14 | | | 0% |
| Integration Test for UAT Environment in Cloud | DCF | 48 | 2 | | | 0% |
| Remediate Faults in UAT Environment | CSP, DCF | 50 | 2 | | | 0% |
| Copy All UAT Environments to Cloud | CSP, DCF | 52 | 1 | | | 0% |
| **Milestone: All UAT Environments Migrated to the Cloud** | | | | | | 0% |
| Install/Configure PROD Mid-Tier Software | DCF | 40 | 2 | | | 0% |
| Refine Detailed Migration Checklist | CSP, DCF | 40 | 2 | | | 0% |
| **Milestone: Production Environment Ready for Migration** | | | | | | 0% |
| Configure PROD LDAP Security | CSP, DCF | 42 | 1 | | | 0% |
| Configure PROD Mid-Tier Databases | CSP, DCF | 42 | 1 | | | 0% |
| Copy Preliminary PROD Environment to Cloud | CSP, DCF | 42 | 1 | | | 0% |
| Integration Test for PROD Environment in Cloud | CSP, DCF | 43 | 3 | | | 0% |
| Configure DR Site | CSP | 43 | 2 | | | 0% |
| Confirm DR Site | CSP | 45 | 2 | | | 0% |
| Copy Supported Platforms Code Stream to PROD in Cloud | CSP, DCF | 52 | 1 | | | 0% |
| Regression Test PROD Environment in Cloud | DCF | 53 | 3 | | | 0% |
| Remediate Faults in PROD Environment | CSP, DCF | 53 | 4 | | | 0% |
| User Acceptance Test PROD Environment in Cloud | CSP, DCF | 56 | 4 | | | 0% |
| **Milestone: Production Environment Confirmed Operational** | | | | | | 0% |
| Create Go Live Checklist (Hour by Hour Plan) | DCF | 57 | 1 | | | 0% |
| Approve Go Live Check List | DCF | 58 | 1 | | | 0% |
| Migration Rehearsal #1 | DCF | 59 | 1 | | | 0% |
| Migration Rehearsal #2 | DCF | 60 | 1 | | | 0% |
| Go/No-Go Check Point | DCF | 61 | 1 | | | 0% |
| **Milestone: Confirmed Proceed With Go-Live** | | | | | | 0% |
| Final Migration/Go Live | DCF | 62 | 1 | | | 0% |
| **Milestone: All Environments Migrated** | | | | | | 0% |
| Cloud Environment Training | CSP, DCF | 57 | 5 | | | 0% |
| Ongoing Cloud Support | CSP | 63 | 263 | | | 0% |

## G. Roles, Responsibilities and Assumptions

The following sections define Roles, Responsibilities and Assumptions related to migrating FSFN to a cloud service provider. The sections define the scope of work and an understanding of expectations related to cloud hosting used to develop the specifications for the cost analysis. Roles, Responsibilities and Assumptions will be divided into the following categories:

1. General
2. Cloud Services Providers
3. Roles, Responsibilities, Staffing
4. Security
5. Hardware
6. Software
7. Networking
8. Service Levels
9. Disaster Recovery and Resiliency

The goal of this section is to define a scope for cloud hosting for FSFN that will provide for continued usability, improved reliability, better support and solid system performance. Each of the following assumptions define the overall scope for migrating FSFN to a cloud service provider. The assumptions were used as factors in the development of estimates for effort and cost.

### 1. General Assumptions

General Assumptions represent roles, responsibilities, and assumptions that impact effort, scope and pricing. These assumptions are not necessarily a fit for one of the other categories of Assumptions in this section.

| Number | Assumption Short Description | Additional Details |
|---|---|---|
| 1. | The system components that make up FSFN will be migrated to the cloud service provider. These components are comprised of the 1) Java Application, 2) Batch, 3) Reporting, 4) ETL, 5) data warehouse and 6) associated databases | No Additional Details |
| 2. | Components utilized by FSFN and shared by other systems will not be migrated to the cloud service provider. These include 1) Address Validation and the 2) Policy Server. | No Additional Details |
| 3. | The migration of FSFN to software platforms that are at supported levels will be completed before FSFN is migrated to the first environment provided by the cloud service provider | Cloud service provider requires FSFN to function on software platforms that are in mainstream support and meet the requirements for the hosting service. FSFN has 92.5% of servers that have software platforms that are out of mainstream support. These platforms will need to be upgraded and FSFN will need to be modified to function on the upgraded software platforms |

| Number | Assumption Short Description | Additional Details |
|---|---|---|
| 4. | A copy of current source code deployed to servers and audit logs and application data will be held in escrow | Source code will continued to be maintained in the DCF ClearCase tool. Copies of the currently deployed compiled code will be provided to DCF. Copies of backups of production databases will be maintained at DCF |
| 5. | Existing Governance Structure will be used to manage the migration of FSFN to a cloud service provider | DCF currently has a detailed governance framework that defines a clear path of approvals and escalation for managing the migration of changes to FSFN. This framework will be used to manage the migration of FSFN to a cloud service provider. |
| 6. | Existing Governance Structure will be used to manage FSFN after the system has been migrated to a cloud service provider | DCF currently has a detailed governance framework that defines a clear path of approvals and escalation for managing the migration of changes to FSFN. This framework will be used to manage the migration of FSFN to a cloud service provider. |

## 2. Cloud Service Providers

The purpose of cloud service provider roles, responsibilities and assumptions is to define what is provided by the service. These assumptions will be used to define gaps in architecture, services and other aspects of system hosting. These gaps will need to be addressed within this plan and outside of the scope of the cloud service provider.

| Number | Assumption Short Description | Additional Details |
|---|---|---|
| 1. | Cloud service provider will provide a Tier 3 Data Center for the primary site. | |
| 2. | Cloud service provider will provide a Tier 3 Data Center for the disaster recovery site | |
| 3. | Cloud service provider will provide virtual machines for middle tier servers | |
| 4. | Cloud service provider will provide LPARs for mainframe hardware | |
| 5. | Cloud service provider will provide hardware that is equal to or better than the hardware currently used for FSFN | |
| 6. | DCF will provide a high bandwidth network connection between the hosting facility and the DCF | |
| 7. | Cloud service provider will provide a HIPAA ready environment | Enforcement of security needs and assessments are the responsibility of DCF |

## 3. Roles, Responsibilities and Staffing

The purpose of the Roles, Responsibilities and Staffing assumptions is to delineate ownership of hosting tasks by the AST, DCF and the cloud service provider. Delineating the ownership of tasks, related to hosting, allows for the creation of more accurate estimates for staff and effort. Creating this delineation also contributes to the creation of Service Level Agreements between each of the participants.

| Number | Assumption Short Description | Additional Details |
|---|---|---|
| 1. | The AST will negotiate the price for the cloud service provider | |
| 2. | DCF will review the proposed Cloud Architecture (Hardware, Software, Network) for FSFN to verify that it meets AST Standards | |
| 3. | DCF will seek the necessary assessments and approvals for the proposed Cloud Architecture (Hardware, Software, Network) for FSFN to verify that it meets state and federal standards | |
| 4. | DCF will manage customer user ID administration for application | |
| 5. | DCF will own disaster recovery plan development and testing | |
| 6. | DCF will own all data and source code related to FSFN. DCF will also be responsible for reviews and audits of logs. | Data includes Application Data, Audit Logs, Reporting Data, Historic Reports and files stored in the database. Source code includes Application Source Code, Report Templates, Document Templates, ETL Source Code and Application Configurations. |

## 4. Security

The purpose of the Security roles, responsibilities and assumptions is to define expectations related to the security of servers, networking and personnel that are involved with FSFN at the cloud service provider. In defining these assumptions, cost estimates can be more accurate for each area impacted by security requirements. These assumptions also contribute to the creations of SLAs related to security.

| Number | Assumption Short Description | Additional Details |
|---|---|---|
| 1. | FSFN contains the following types of data: PII, HIPAA, Medicaid and CJIS | |
| 2. | DCF is responsible for performing assessments and obtaining approvals needed to meet federal and state regulations for FSFN | |

## 5. Hardware

The purpose of Hardware assumptions is to define responsibilities related to the hardware that will be used by FSFN at the cloud service provider. By defining these responsibilities, a more accurate estimate for cost and effort was developed. These assumptions also contribute to the creation of SLAs related to hardware.

### *Middle Tier*

The following assumptions are specific to middle tier server hardware.

| Number | Assumption Short Description | Additional Details |
|---|---|---|
| 1. | The cloud service provider will provide computing hardware that is N to N-1 with regard to currency of vendor supported platforms. | This means that the hardware used for hosting will be between the current version or one version back based on the product line provided by the hardware vendor |
| 2. | The cloud service provider will provide patching and upgrades for computing hardware in the Cloud Data Center | |

### *Mainframe*

The following assumptions are specific to mainframe hardware.

| Number | Assumption Short Description | Additional Details |
|---|---|---|
| 1. | The cloud service provider will provide mainframe computing hardware equivalent to that currently hosted by the AST for FSFN | |
| 2. | The cloud service provider will provide patching and upgrades for mainframe in Cloud Data Center | |

## 6. Software

The purpose of Software assumptions is to define responsibilities related to the software that will be used by FSFN at the cloud service provider. By defining these responsibilities, a more accurate estimate for cost and effort was developed. These assumptions also contribute to the creation of SLAs related to software and developed code.

| Number | Assumption Short Description | Additional Details |
|---|---|---|
| 1. | The cloud service provider will support commercially current and available operating systems for x86 including Redhat Enterprise Linux, Microsoft Windows Server and IBM AIX. | For the purpose of the cost analysis, it is expected that the cloud service provider will provide the operating system as part of the Virtual Machine provided |
| 2. | The cloud service provider will be responsible for patching operating systems to current supported levels | The cloud service provider will provide ongoing patching for operating systems managed by the provider |
| 3. | For mainframe, all IBM software products will be included with the cost of the mainframe service | This includes the operating system and the database |

| Number | Assumption Short Description | Additional Details |
|---|---|---|
| 4. | For middle tier all software licenses for FSFN, except for operating system, will be provided or purchased for installation in the cloud | The list of software consists of:<br>Java Enterprise Edition 7<br>IBM WebSphere ND 8.5<br>SAP BOE 4.1<br>SAP BO DS 4.2<br>IBM DB2 LUW 10.x |
| 5. | FSFN will be on software platforms that are in mainstream support before migration to a cloud service provider | |

## 7. Networking

The purpose of Networking assumptions is to define expectations related to the networking infrastructure that will be used by FSFN at the cloud service provider. By defining these assumptions, a more accurate cost estimate was developed for each segment of the network provided by each of the participating agencies (DCF, AST and cloud service provider). These assumptions also contribute to the creation of SLAs related to networking.

| Number | Assumption Short Description | Additional Details |
|---|---|---|
| 1. | Users will access FSFN in the cloud through the existing VPN solution | |
| 2. | The state will provide network connectivity from DCF to the cloud service provider primary and disaster recovery site | |

## 8. Service Levels

The purpose of the Service Level assumptions is to provide expectations for system availability, performance, reliability and changes. These assumptions also define the expectations for each of the participants in the cloud hosting effort.

| Number | Assumption Short Description | Additional Details |
|---|---|---|
| 1. | The Production Virtual Machines supporting FSFN will be maintained at the equivalent of 99.9% up time or better | |
| 2. | Outages and Issues related to Virtual Machines will have SLA response times based on severity | |
| 3. | Application Support Services will have SLAs related to the performance and availability of application components, such as reporting, batch and application servers | |

## 9. Disaster Recovery and Resiliency

The purpose of Disaster Recovery and Resiliency assumptions is to create the expectations for these services for FSFN after it is moved to a cloud service provider. These assumptions define the expectations as they related to each of the participants (AST, DCF, cloud service provider) in the cloud hosting effort for FSFN.

| Number | Assumption Short Description | Additional Details |
|---|---|---|
| 1. | A syndicated mainframe will be available within 24 hours of the declaration of a disaster | |
| 2. | Production middle tier servers will be available within 4 hours of the declaration of a disaster | |
| 3. | Data and servers are replicated in 15 minute intervals | |
| 4. | System recovery is achievable within 36 hours | |

# H. Federal Regulations Related to Hosting in a Cloud Environment

FSFN System is a federally funded Statewide Automated Child Welfare Information System (SACWIS) used for case administration and management. As such, FSFN is Florida's system of record for all children and families receiving child welfare support and contains complete case management history. The federal SACWIS program is managed by the Children's Bureau, which is an office of the Administration of Children and Families (ACF), Department of Health and Human Services.

Given the fact that 1) FSFN is funded, in part, by the federal SACWIS Program and 2) FSFN manages child welfare records, there are a number of regulations and guidelines that are directly applicable to FSFN that need to be addressed prior to migration to the cloud. The applicable areas to be addressed prior to the migration are discussed in the following paragraphs and the specific actions to address each are highlighted:

- Health Insurance Portability and Accountability Act (HIPAA)
- Criminal Justice Information Services (CJIS) Security Policy v5.3
- ACF Children's Bureau, Advanced Planning Document (APD)
- Centers for Medicare and Medicaid Services (CMS)
- Federal Risk and Authorization Management Program (FedRAMP)

## 1. Health Insurance Portability and Accountability Act (HIPAA)

The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses and those health care providers that conduct certain health care transactions electronically.

The Rule requires appropriate safeguards to protect the privacy of personal health information and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization.

FSFN currently falls under the HIPAA Rule, and will continue to do so. The selected cloud service provider would be required to provide a HIPAA compliant IaaS, and that requirement as well as the associated costs have been factored into the information provided in this Plan.

## 2. Criminal Justice Information Services (CJIS) Security Policy v5.3

The CJIS Security Policy provides Criminal Justice Agencies (CJA) and Noncriminal Justice Agencies (NCJA) with a minimum set of security requirements for access to Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division systems and information and to protect and safeguard Criminal Justice Information (CJI). This minimum standard of security requirements ensures continuity of information protection. The essential premise of the CJIS Security Policy is to provide the appropriate controls to protect CJI from creation through dissemination, whether at rest or in transit.

The CJIS Security Policy applies to all entities with access to, or who operate in support of, FBI CJIS Division's services and information. The CJIS Security Policy provides minimum security requirements associated with the creation, viewing, modification, transmission, dissemination, storage or destruction of CJI. FSFN stores Criminal Background summary data within the system and, as such, the CJIS Security Policy is applicable.

Specifically, FSFN provides access to a Policy Server, which houses background check information. This is the primary data that would apply to the CJIS Security Policy. This background check information is temporarily available for 72 hours after request. The detailed data is not stored in FSFN. A FSFN user can document (using a Yes/No flag) the existence of a criminal background for a specified individual.

To address the CJIS Security Policy, coordination and approval may be required from the Florida Department of Law Enforcement (FDLE) to move FSFN to the cloud. We anticipate that the same agreements that are in place

today to handle potential CJIS data transmission will need to be in place with the external cloud provider. To mitigate risks associated with CJIS data the proposed plan to move FSFN to the cloud was architected so:

- The Policy Server, which houses background check information, would continue to be hosted in its current location. The detailed Criminal Background data would not leave the state's facilities.
- The CJIS data that would be stored within the cloud service provider's facilities is clearly identified.
- Cloud service provider's staff that would have access to the CJIS data are identified; per this plan the only staff that may access CJIS data is the Physical DBA.
- The cloud service provider would need to verify that staff would be required to sign the security addendum and take CJIS security awareness training.

### 3. Centers for Medicare and Medicaid Services (CMS)

Like the Administration for Children and Families (ACF) the federal organization administering the SACWIS program, the Centers for Medicare and Medicaid Services (CMS) is part of the Department of Health and Human Services. CMS is noted for the fact that it "disseminates more data than almost any other federal agency or public company", and due to the mission of CMS, this includes both PII and PHI data. This is relevant to the FSFN Cloud Hosting Plan because CMS has 1) recognized the movement toward cloud hosting and 2) published internal procedures for CMS programs to follow when migrating to the cloud.

To begin, CMS recognizes the shift within the technical environment making cloud hosting viable options for its internal systems. In recent publications, CMS acknowledges that the use of cloud hosting "could provide CMS with greater operational capacity and flexibility while offering increased agility in developing agency capabilities." Furthermore, CMS has stated that it "supports the use of cloud computing services and components that cost effectively delivers needed efficiencies for our internal and external stakeholders."

To address the movement towards cloud hosting, CMS has published guidance for CMS Business and Program stakeholders in the use of cloud computing technology services. This is predicated on the CMS observation that "there are varying degrees of maturity for cloud services and cloud service providers." To address the various in cloud maturity, CMS has published guidance, which centers on adherence to the Federal Risk and Authorization Management Program (FedRAMP). Accordingly, it is recommended that DCF include a FedRAMP assessment within the Implementation Plan. Further details regarding FedRAMP are included in Section 6.4, which immediately follows below.

### 4. Federal Risk and Authorization Management Program (FedRAMP)

The final applicable federal guideline involves the Federal Risk and Authorization Management Program, or FedRAMP. FedRAMP is a Federal program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP is the result of close collaboration with cybersecurity and cloud experts from the General Services Administration (GSA), National Institute of Standards and Technology (NIST), Department of Homeland Security (DHS), Department of Defense (DOD), National Security Agency (NSA), Office of Management and Budget (OMB), the Federal Chief Information Officer (CIO) Council and its working groups, as well as private industry.

While FedRAMP framework was designed specifically for Federal agencies requesting Cloud Infrastructures, FedRAMP defines guidelines, primarily the Security Assessment, which the State should also apply the FSFN cloud migration. Appendix C, Attachments, contains the FedRAMP Security Assessment Framework to be completed prior to the migration.

### 5. Children's Bureau - Advanced Planning Document (APD)

Once HIPAA, CJIS, Medicaid and FedRAMP policies have been addressed and the appropriate approvals are in place, an Advanced Planning Document (APD) needs to be completed and filed with Administration for Children and Families (ACF) The Children's Bureau.

Moving FSFN to a cloud service provider would need to be documented in a planning and implementation APD. The APD document filed would provide the information regarding changes or modifications to FSFN, the organization supporting the system, and the associated costs incurred by the State.

# Appendix A – Acronyms

The table below provides the descriptions abbreviated by acronyms referenced in this document.

| ACRONYM | DESCRIPTION |
|---|---|
| ACF | Administration for Children and Families |
| AEM | Adobe Experience Manager |
| AHCA | Agency for Health Care Administration |
| APD | Advanced Planning Document |
| AST | Agency for State Technology |
| ATO | Authorization to Operate |
| BI | Business Intelligence |
| BLOB | Binary Large OBject |
| BOE/BO | Business Objects Enterprise |
| CBC | Community Based Care |
| CIO | Chief Information Officer |
| CJA | Criminal Justice Agencies |
| CJI | Criminal Justice Information |
| CJIS | Criminal Justice Information Services |
| CMS | Centers for Medicare and Medicaid Services |
| CMS | Content Management System |
| COBOL | Common Business-Oriented Language |
| COTS | Commercial Off The Shelf |
| CRM | Customer Relationship Management |
| CRX | Content Repository eXtreme |
| CSP | Cloud Service Provider |
| CSS | Cascading Style Sheet |
| CTI | Computer Telephony Integration |
| DAO | Data Access Object |

| ACRONYM | DESCRIPTION |
|---|---|
| DCF | Florida Department of Children and Families |
| DCUT | Design, Code, Unit Test |
| DHS | Department of Homeland Security |
| DOD | Department of Defense |
| DR | Disaster Recovery |
| DS | Data Services |
| EDMS | Electronic Document Management System |
| ESB | Enterprise Service Bus |
| ETL | Extract Transform Load |
| FAQ | Frequently Asked Question |
| FBI | Federal Bureau of Investigation |
| FDLE | Florida Department of Law Enforcement |
| FedRAMP | Federal Risk and Authorization Management Program |
| FSFN | Florida Safe Families Network |
| GIS | Graphical Information System |
| GSA | General Services Administration |
| HIPAA | Health Insurance Portability and Accountability Act |
| HTML | Hypertext Markup Language |
| IaaS | Infrastructure as a Service |
| ICBN | Integrate Critical Business Needs |
| ICPC | Interstate Compact on the Placement of Children |
| ICS | Interstate Compact System |
| IDAA | IBM DB2 Analytics Accelerator |
| ISV | Independent Software Vendor |
| ITIL | Information Technology Infrastructure Library |

| ACRONYM | DESCRIPTION |
|---|---|
| IVR | Interactive Voice Response |
| JAB | Joint Authorization Board |
| JCL | Job Control Language |
| JDBC | Java Database Connectivity |
| JMS | Java Messaging Service |
| JSP | Java Server Page |
| LCMS | Learning Content Management System |
| LDAP | Lightweight Directory Access Protocol |
| LPAR | Logical Partition |
| LOB | Large Object |
| LUW | Linux, Unix, Windows |
| M&O | Maintenance and Operations |
| MVC | Model View Controller |
| NCJA | Noncriminal Justice Agencies |
| NEICE | National Electronic Interstate Compact Enterprise System |
| N-1 | Current Major Version Minus One (Software Platform) |
| NIST | National Institute of Standards and Technology |
| NSA | National Security Agency |
| OCW | Office of Child Welfare |
| OLAP | Online Analytical Processing |
| OLTP | Online Transaction Processing |
| OMB | Office of Management and Budget |
| PaaS | Platform as a Service |
| PHI | Personal Health Information |
| PII | Personally Identifiable Information |

| ACRONYM | DESCRIPTION |
|---|---|
| PMO | Project Management Office |
| PVU | Processor Value Unit |
| R&MA/RMA | Recover and Maintain Architecture |
| RDC | Remote Data Capture |
| RFT | Rational Functional Tester |
| RHEL | RedHat Enterprise Linux |
| RPT | Rational Performance Tester |
| RTF | Rich Text Format |
| RPO | Recovery Point Objective |
| RTO | Recovery Time Objective |
| SACWIS | Statewide Automated Child Welfare Information System |
| SaaS | Software as a Service |
| SAN | Storage Area Network |
| SLA | Service Level Agreement |
| SM&O/SMO | Support Maintenance and Operations |
| TBD | To Be Determined |
| UAT | User Acceptance Test |
| VPN | Virtual Private Network |
| XML | eXtended Markup Language |
| XSD | XML Schema Definition |

# Appendix B – Glossary

The table below provides definitions for specific terms and words referenced in this document.

| TERM | DEFINITION |
|---|---|
| ALM | See application lifecycle management |
| API | See application programming interface |
| application lifecycle management (ALM) | An iterative and continuous process of coordinating people, processes and tools with the goal of delivering a software or systems project. This process involves planning and change management, requirements definition and management, architecture management, software configuration management, build and deployment automation, application security and quality management. The features of this process include traceability across lifecycle artifacts, process definition and enactment, and reporting. |
| application programming interface (API) | An interface that allows an application program that is written in a high-level language to use specific data or functions of the operating system or another program. |
| autonomic | Pertaining to an on-demand operating environment that responds automatically to problems, security threats, and system failures. |
| bare metal | Pertaining to a computer or network independent of its operating system or hypervisor. See also virtualization. |
| broad network access | Capabilities are available over the network and accessed through standard mechanisms that promote heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations) |
| cloud | A network that delivers requested virtual resources as a service. |
| cloud application | An application that is extended to be accessible through the Internet. Cloud applications use large data centers and powerful servers that host web applications and web services. |
| cloud client | Software or hardware that is designed to deliver cloud services or that relies on cloud computing to operate. |
| cloud computing | A computing platform where users can have access to applications or computing resources as services from anywhere through their connected devices. A simplified user interface or application programming interface (API), or both, make the infrastructure supporting such services transparent to users. See also off-premises. |
| cloud infrastructure | See infrastructure as a service |
| cloud provider | An organization that provides cloud computing resources |
| cloud service provider (CSP) | A service provider that offers storage or software services or solutions through a public, private, or hybrid cloud |
| cloud storage | A storage resource provided by a cloud, or the storage of data on virtual public or private servers in the cloud |

| | |
|---|---|
| cloud-enabled | Pertaining to a model or implementation of a public, private or hybrid cloud environment |
| community cloud | The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy and compliance considerations). It may be owned, managed and operated by one or more of the organizations in the community, a third party or some combination of them, and it may exist on or off premises |
| connection broker | An intermediary program that assigns a user to an available virtual desktop upon request |
| container | A virtual software object that encompasses all of the elements that are needed for an application to run within an operating system |
| CSP | See cloud service provider |
| DevOps | A software methodology that integrates application development and IT operations |
| disaster recovery | Recovery of the use of an application from an outage |
| external cloud | See public cloud |
| hosted private cloud | A cloud computing environment that is owned and operated by the same company. The customer owns and pays for infrastructure and has unlimited exclusive access. |
| hybrid cloud | A cloud computing environment that consists of multiple public and private resources |
| IaaS | See infrastructure as a service |
| infrastructure as a service (IaaS) | The delivery of a computer infrastructure, including server functionality, networking functionality, data center functionality and storage functionality as an outsourced service |
| internal cloud | See private cloud |
| managed private cloud | A cloud computing environment that is enterprise owned and operated by another company. The customer owns and pays for infrastructure and has unlimited exclusive access. |
| measured service | Cloud systems automatically control and optimize resource use by leveraging a metering capability (ability to track usage, activity or other infrastructure related metrics) at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth and active user accounts). Resource usage can be monitored, controlled and reported, providing transparency for both the provider and consumer of the utilized service. |
| middleware | Software that acts as an intermediate layer between applications or between client and server. It is used most often to support complex, distributed applications in heterogeneous environments. |
| middle tier | Hardware related to non-mainframe computing resources |

| | |
|---|---|
| mid-tier | See middle tier |
| mobile cloud | An infrastructure in which the storage and processing of data for applications is offloaded from a mobile device into the cloud. With mobile cloud computing, applications are not limited to a specific carrier but are accessed through the Web. |
| multitenancy | The ability to deliver software to multiple client organizations from a single, shared instance of the software |
| off-premises | Pertaining to software that is accessed through a remote computer or over the Internet. See also cloud computing |
| on-demand self service | Means that a consumer can unilaterally provision computing capabilities (e.g., server time and network storage) automatically, as needed, without requiring human interaction with each service provider |
| on-prem | See on-premises. |
| on-premises (on-prem) | Pertaining to software that is installed and run on the local computers of a user or organization |
| PaaS | See platform as a service |
| peer-to-peer | Pertaining to a form of distributed processing in which the front-end and back-end of a conversation switch control between themselves. It is communication between equals. |
| platform as a service (PaaS) | The delivery of a computing platform; including applications, optimized middleware, development tools, Java and Web 2.0 runtime environments; in a cloud-based environment. |
| point of presence (PoP) | A physical location that stores servers and routers in a network cloud |
| PoP | See point of presence |
| private cloud | A cloud computing environment in which access is limited to members of an enterprise and partner networks |
| provisioning | The process of making computing resources available to users |
| public cloud | A cloud computing environment in which access to standardized resources owned and managed by a service provider is permitted to subscribers on a pay-per-use basis |
| rapid elasticity | Capabilities can be elastically (rapidly adding or removing virtual machines, processors, memory or storage) provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time. |
| resource pooling | The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources (e.g., virtual machines, storage, or network) |

| | |
|---|---|
| | but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory and network bandwidth. |
| runtime | The set of resources used to run the application |
| SaaS | See software as a service |
| scalability | The ability of a system to expand as resources, such as processors, memory or storage, are added |
| service | A cloud extension that provides ready-for-use functionality, such as database, messaging and web software for running code, or application management or monitoring capabilities. Services usually do not require installation or maintenance and can be combined to create applications. |
| service level agreement | Defined metrics for assessing the performance of an application |
| service-oriented architecture (SOA) | A conceptual description of the structure of a software system in terms of its components and the services they provide without regard for the underlying implementation of these components, services and connections between components. |
| shared private cloud | A cloud computing environment in which a company owns the infrastructure and the customer has shared access and pays per usage |
| SLA | See service level agreement |
| SOA | See service-oriented architecture |
| software as a service (SaaS) | A model of software deployment whereby software including business processes, enterprise applications and collaboration tools, are provided as a service to customers through the cloud. |
| system of engagement | An information technology (IT) system that incorporates technologies that encourage user interaction through email, collaboration systems and networking. A system of engagement often uses cloud technologies to extend the usefulness of systems of record. |
| utility computing | A usage model in which customers pay for computational resources through an established fee-per-time schedule |
| virtual machine (VM) | A software implementation of a machine that executes programs like a real machine |
| virtual private cloud | A private cloud that exists within a public cloud and is accessed through a virtual private network (VPN) |
| virtualization | The substitution of virtual resources for actual resources where the virtual resources have the same functions and external interfaces as their counterparts, but differ in attributes, such as size, performance and cost. Virtualization is commonly applied to physical hardware resources by combining multiple physical resources into shared pools from which users receive virtual resources. See also bare metal, grid computing. |
| VM | See virtual machine |

# Appendix C - Federal Risk and Authorization Management Program (FedRAMP) – Security Assessment Framework

The following attachment is the security assessment framework for the FedRAMP Program. This attachment is associated with Section 6, Federal Regulations Related to Hosting in a Cloud Environment,.

FedRAMP-Security-Assessment-Framew

# Appendix D - Centers for Medicare and Medicaid Services (CMS) – Computing Policy

The following attachment is the complete Centers for Medicare and Medicaid Services Computing Policy.

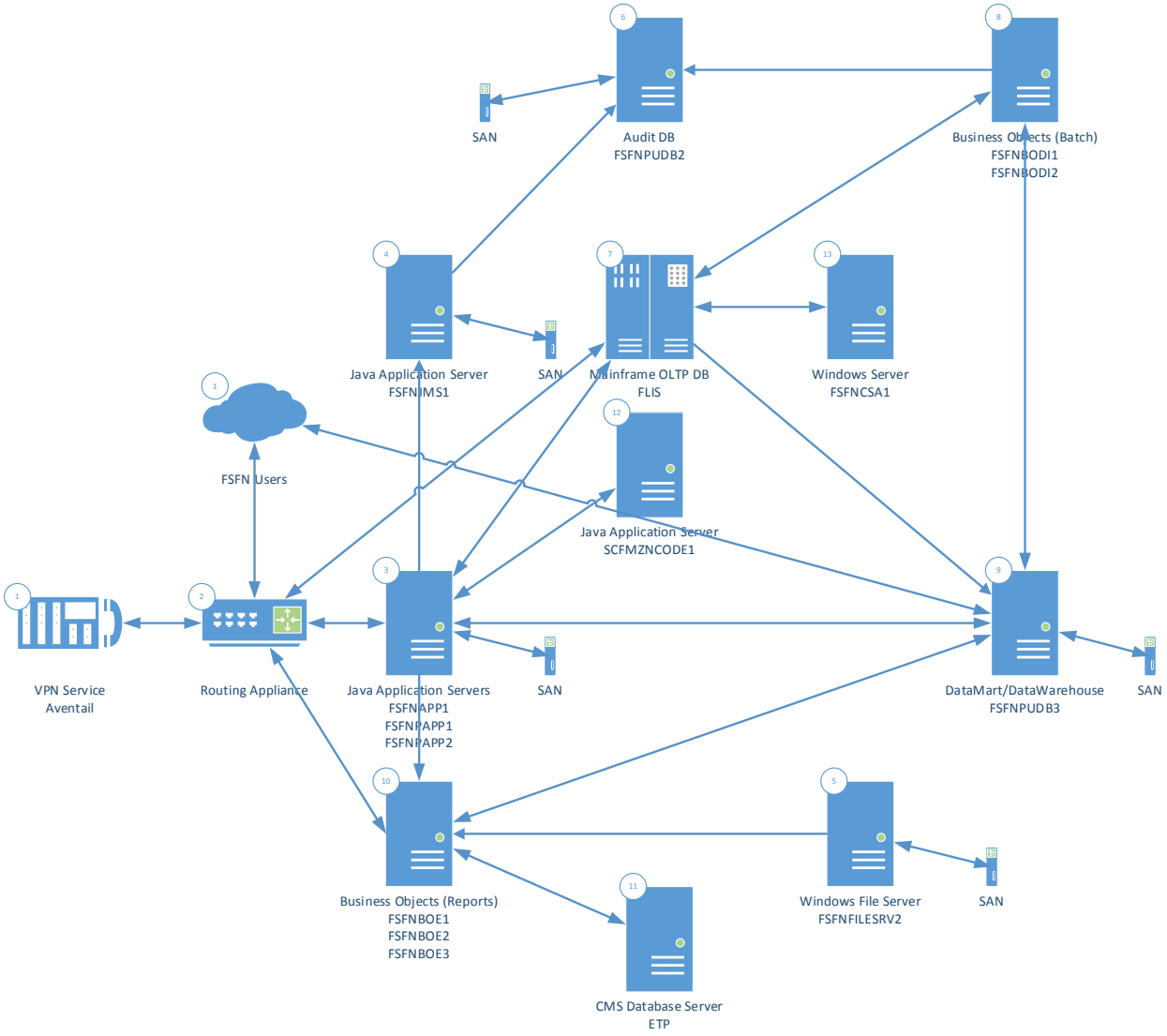
CMS Policy_for_Cloud_Co

# Appendix E – FSFN System Architecture/Inventory

FSFN is comprised of two distinct applications: the FSFN Case Management system and the Abuse Portal. The FSFN Case Management System is the primary application used by DCF, the CBCs and other partners. It is a custom application with a SAP Business Objects data warehouse that has been built to support the Florida's unique child welfare environment. The second system is the Abuse Hotline Portal which is integrated closely with FSFN, built on the Microsoft Dynamics platform and used by the public and the DCF Abuse Reporting Call Center.

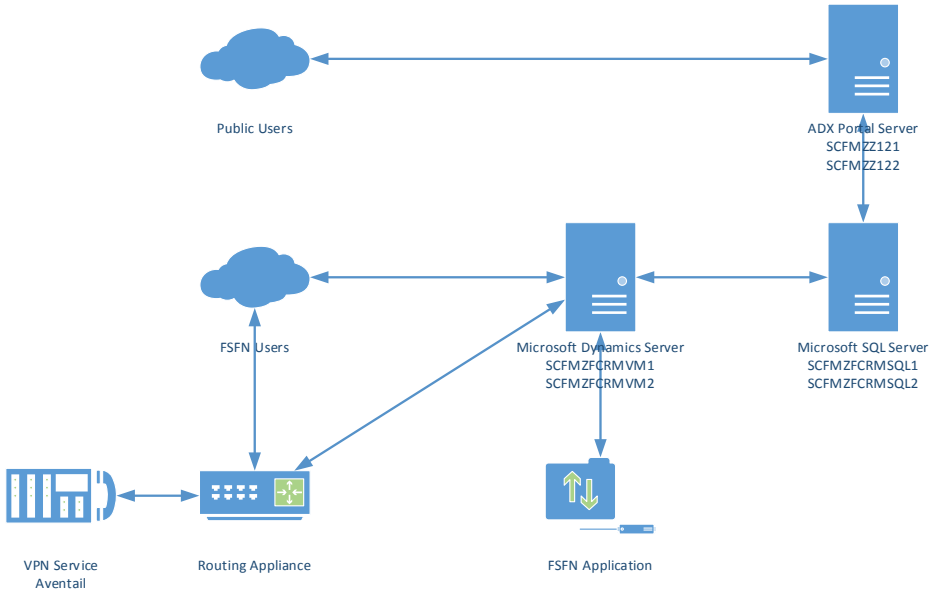
FSFN (both Case Management and Portal) is web based, highly customized, adapted to the Florida's needs and comprised of over 2,000 feature-rich screens. These screens provide users with the ability to initiate and manage cases, investigations, adoptions, placements, services, Medicaid and much more. A robust reporting system that provides a standardized data structure for creating custom reports, as well as standardized daily, weekly and monthly reports, supports these functions. The application also has multiple interfaces that export and import data with other systems such as the FLORIDA System, the Juvenile Justice Information System, Agency for Health Care Administration (AHCA) databases and the federal Children's Bureau.

FSFN is a multi-tier application that separates the web, application and data layers. This architecture enables high security (given the sensitivity of the data that resides in the system) and optimization of performance at multiple levels. FSFN runs on a mixture of mainframe and middle tier servers. The mainframe hosts a DB2 Database which holds over 30 years of Florida Child Welfare data. The mainframe is currently shared with the FLORIDA system which utilizes approximately 70% of the overall capacity, leaving FSFN with the remaining 30%. The remainder of the system (the web and application services) operates on Intel based middle tier servers. There are 57 servers (across all environments) that provide the hardware for running the application, reporting, interfaces and other features of the system. The following diagram shows a high level view of the Production Environment for FSFN.




## 1. Production FSFN System Technical Architecture

In addition to FSFN, there is the Abuse Hotline Portal. This system runs independently of FSFN and is used to capture both child and adult abuse cases for investigation. Cases are entered either through the Hotline Portal by agency staff or by the public through the Abuse Portal. Cases are transferred, through interfaces, to FSFN where the cases are created and assigned to a case worker. The Abuse Hotline Portal operates on 16 middle tier servers, providing the hardware for running the hotline application, portal and supporting databases. The following diagram shows a high-level view of the Production Environment for the Abuse Hotline Portal.




**Production Abuse Hotline Portal Technical Architecture**

## 2. Environment Inventory

The following sections represent an initial assessment of the Hardware and Software inventories needed to support migration of FSFN to the cloud service provider. This inventory was used to estimate costs listed in the cost benefit analysis.

### *Infrastructure as a Service (Hybrid/Blended Hosting Option)*

The list of hardware and software in this section is related to FSFN using mainframe and middle tier hardware in the implementation.

#### Mainframe

The following are the details for the mainframe hardware and software needed to support FSFN.

##### *Hardware*

| Environment | Processors | Storage |
|---|---|---|
| All | 120 MSU<br>960 MIPS | 9,000 GB DASD |

| Backup Hardware | Sizing |
|---|---|
| All | 84,000 GB Virtual Tape Library |

##### *Software*

| Independent Software Vendors (ISVs) |
|---|
| Enterprise COBOL for zOS |
| Netview File Transfer Program V2 |
| PC File Transfer Program |
| DB2 for zOS v10 |

##### *Middle Tier Servers*

The following are the details for the middle tier hardware and software needed to support FSFN.

| Environment | Server | Cores | Memory | Storage | Software |
|---|---|---|---|---|---|
| Development | Report Server | 4 (64 Bit) | 32GB | 500GB | RHEL 7.x (64 Bit)<br>SAP BOE 4.1.x |
| Development | Data Warehouse and Data Mart | 4 (64 Bit) | 16GB | 7.2TB | RHEL 7.x (64 Bit)<br>IBM DB2 LUW 10.5 |

| Environment | Server | Cores | Memory | Storage | Software |
|---|---|---|---|---|---|
| Test | Report Server | 4 (64 Bit) | 32GB | 500GB | RHEL 7.x (64 Bit)<br>SAP BOE 4.1.x |
| Test | Data Warehouse and Data Mart | 4 (64 Bit) | 16GB | 7.2TB | RHEL 7.x (64 Bit)<br>IBM DB2 LUW 10.5 |
| UAT | Report Server | 4 (64 Bit) | 32GB | 100GB | RHEL 7.x (64 Bit)<br>SAP BOE 4.1.x |
| UAT | Report Server | 4 (64 Bit) | 32GB | 100GB | RHEL 7.x (64 Bit)<br>SAP BOE 4.1.x |
| UAT | File Server | 2 (64 Bit) | 8GB | 500GB | RHEL 7.x (64 Bit) |
| UAT | Data Warehouse and Data Mart | 8 (64 Bit) | 64GB | 12TB | RHEL 7.x (64 Bit)<br>IBM DB2 LUW 10.5 |
| Production | Report Server | 4 (64 Bit) | 64GB | 100GB | RHEL 7.x (64 Bit)<br>SAP BOE 4.1.x |
| Production | Report Server | 4 (64 Bit) | 64GB | 100GB | RHEL 7.x (64 Bit)<br>SAP BOE 4.1.x |
| Production | Report Server | 4 (64 Bit) | 64GB | 100GB | RHEL 7.x (64 Bit)<br>SAP BOE 4.1.x |
| Production | File Server | 2 (64 Bit) | 8GB | 5TB | RHEL 7.x (64 Bit) |
| Production | Data Warehouse and Data Mart | 12 (64 Bit) | 128GB | 1.5TB | RHEL 7.x (64 Bit)<br>IBM DB2 LUW 10.5 Enterprise |
| Development | ETL Server | 4 (64 Bit) | 32GB | 1TB | RHEL 7.x (64 Bit)<br>SAP DS 4.2.x |
| Test | ETL Server | 4 (64 Bit) | 32GB | 1TB | RHEL 7.x (64 Bit)<br>SAP DS 4.2.x |
| UAT | ETL Server | 4 (64 Bit) | 64GB | 1TB | RHEL 7.x (64 Bit)<br>SAP DS 4.2.x |
| UAT | ETL Server | 4 (64 Bit) | 64GB | 1TB | RHEL 7.x (64 Bit)<br>SAP DS 4.2.x |

| Environment | Server | Cores | Memory | Storage | Software |
|---|---|---|---|---|---|
| Production | ETL Server | 4 (64 Bit) | 64GB | 100GB | RHEL 7.x (64 Bit)<br>SAP DS 4.2.x |
| Production | ETL Server | 4 (64 Bit) | 64GB | 100GB | RHEL 7.x (64 Bit)<br>SAP DS 4.2.x |
| Development | Application Server | 8 (64 Bit) | 32GB | 200GB | RHEL 7.x (64 Bit)<br>WebSphere ND 8.5 |
| Development | Audit Database | 4 (64 Bit) | 32GB | 4TB | RHEL 7.x (64 Bit)<br>IBM DB2 LUW 10.5 |
| Test | Application Server | 8 (64 Bit) | 32GB | 200GB | RHEL 7.x (64 Bit)<br>WebSphere ND 8.5 |
| Test | Audit Database | 4 (64 Bit) | 32GB | 4TB | RHEL 7.x (64 Bit)<br>IBM DB2 LUW 10.5 |
| UAT | Application Server | 8 (64 Bit) | 64GB | 200GB | RHEL 7.x (64 Bit)<br>WebSphere ND 8.5 |
| UAT | Application Server | 8 (64 Bit) | 64GB | 200GB | RHEL 7.x (64 Bit)<br>WebSphere ND 8.5 |
| UAT | Audit Database | 8 (64 Bit) | 64GB | 4TB | RHEL 7.x (64 Bit)<br>IBM DB2 LUW 10.5 |
| Production | Application Server | 8 (64 Bit) | 64GB | 500GB | RHEL 7.x (64 Bit)<br>WebSphere ND 8.5 |
| Production | Application Server | 8 (64 Bit) | 64GB | 500GB | RHEL 7.x (64 Bit)<br>WebSphere ND 8.5 |
| Production | Application Server | 8 (64 Bit) | 64GB | 500GB | RHEL 7.x (64 Bit)<br>WebSphere ND 8.5 |
| Production | Application Server | 8 (64 Bit) | 64GB | 500GB | RHEL 7.x (64 Bit)<br>WebSphere ND 8.5 |
| Production | Audit Database | 8 (64 Bit) | 64GB | 20TB | RHEL 7.x (64 Bit)<br>IBM DB2 LUW 10.5 Enterprise |

| Environment | Server | Cores | Memory | Storage | Software |
|---|---|---|---|---|---|
| Production | CRM App Server | 8 (64 Bit) | 16GB | 1600GB | Windows Server 2012 R2 Data Center Edition<br>Microsoft CRM 2010 |
| Production | CRM Database | 4 (64 Bit) | 8GB | 1600GB | Windows Server 2012 R2 Data Center Edition<br>MS SQL Server |
| Production | CRM Web Server | 4 (64 Bit) | 4GB | 164GB | Windows Server 2012 R2 Data Center Edition<br>ADX Studio |
| Production | CRM App Server | 8 (64 Bit) | 16GB | 1600GB | Windows Server 2012 R2 Data Center Edition<br>Microsoft CRM 2010 |
| Production | CRM Database | 4 (64 Bit) | 8GB | 1600GB | Windows Server 2012 R2 Data Center Edition<br>MS SQL Server |
| Production | CRM Web Server | 4 (64 Bit) | 4GB | 164GB | Windows Server 2012 R2 Data Center Edition<br>ADX Studio |
| Test | CRM App Server | 4 (64 Bit) | 8GB | 164GB | Windows Server 2012 R2 Data Center Edition<br>Microsoft CRM 2010 |
| Test | CRM Database | 4 (64 Bit) | 8GB | 164GB | Windows Server 2012 R2 Data Center Edition<br>MS SQL Server |
| Test | CRM Web Server | 4 (64 Bit) | 4GB | 164GB | Windows Server 2012 R2 Data Center Edition<br>ADX Studio |
| Test | CRM App Server | 4 (64 Bit) | 8GB | 164GB | Windows Server 2012 R2 Data Center Edition<br>Microsoft CRM 2010 |
| Test | CRM Database | 4 (64 Bit) | 8GB | 164GB | Windows Server 2012 R2 Data Center Edition<br>MS SQL Server |

| Environment | Server | Cores | Memory | Storage | Software |
|---|---|---|---|---|---|
| Test | CRM Web Server | 4 (64 Bit) | 4GB | 164GB | Windows Server 2012 R2 Data Center Edition<br>ADX Studio |
| Development | CRM App Server | 2 (64 Bit) | 4GB | 164GB | Windows Server 2012 R2 Data Center Edition<br>Microsoft CRM 2010<br>ADX Studio |
| Development | CRM Database | 2 (64 Bit) | 4GB | 164GB | Windows Server 2012 R2 Data Center Edition<br>MS SQL Server |
| Training | CRM App Server | 2 (64 Bit) | 4GB | 164GB | Windows Server 2012 R2 Data Center Edition<br>Microsoft CRM 2010 |
| Training | CRM Database | 2 (64 Bit) | 4GB | 164GB | Windows Server 2012 R2 Data Center Edition<br>MS SQL Server |
| Training | CRM Web Server | 2 (64 Bit) | 4GB | 164GB | Windows Server 2012 R2 Data Center Edition<br>ADX Studio |

### Infrastructure as a Service (Mid-Tier Hosting Option)

The list of hardware and software in this section is related to FSFN using only middle tier hardware in the implementation.

| Environment | Server | Cores | Memory | Storage | Software |
|---|---|---|---|---|---|
| Development | Report Server | 4 (64 Bit) | 32GB | 500GB | RHEL 7.x (64 Bit)<br>SAP BOE 4.1.x |
| Development | Data Warehouse and Data Mart | 4 (64 Bit) | 16GB | 7.2TB | RHEL 7.x (64 Bit)<br>IBM DB2 LUW 10.5 |
| Test | Report Server | 4 (64 Bit) | 32GB | 500GB | RHEL 7.x (64 Bit)<br>SAP BOE 4.1.x |
| Test | Data Warehouse and Data Mart | 4 (64 Bit) | 16GB | 7.2TB | RHEL 7.x (64 Bit)<br>IBM DB2 LUW 10.5 |

| Environment | Server | Cores | Memory | Storage | Software |
|---|---|---|---|---|---|
| UAT | Report Server | 4 (64 Bit) | 32GB | 100GB | RHEL 7.x (64 Bit)<br>SAP BOE 4.1.x |
| UAT | Report Server | 4 (64 Bit) | 32GB | 100GB | RHEL 7.x (64 Bit)<br>SAP BOE 4.1.x |
| UAT | File Server | 2 (64 Bit) | 8GB | 500GB | RHEL 7.x (64 Bit) |
| UAT | Data Warehouse and Data Mart | 8 (64 Bit) | 64GB | 12TB | RHEL 7.x (64 Bit)<br>IBM DB2 LUW 10.5 |
| Production | Report Server | 4 (64 Bit) | 64GB | 100GB | RHEL 7.x (64 Bit)<br>SAP BOE 4.1.x |
| Production | Report Server | 4 (64 Bit) | 64GB | 100GB | RHEL 7.x (64 Bit)<br>SAP BOE 4.1.x |
| Production | Report Server | 4 (64 Bit) | 64GB | 100GB | RHEL 7.x (64 Bit)<br>SAP BOE 4.1.x |
| Production | File Server | 2 (64 Bit) | 8GB | 5TB | RHEL 7.x (64 Bit) |
| Production | Data Warehouse and Data Mart | 12 (64 Bit) | 128GB | 1.5TB | RHEL 7.x (64 Bit)<br>IBM DB2 LUW 10.5 Enterprise |
| Development | ETL Server | 4 (64 Bit) | 32GB | 1TB | RHEL 7.x (64 Bit)<br>SAP DS 4.2.x |
| Test | ETL Server | 4 (64 Bit) | 32GB | 1TB | RHEL 7.x (64 Bit)<br>SAP DS 4.2.x |
| UAT | ETL Server | 4 (64 Bit) | 64GB | 1TB | RHEL 7.x (64 Bit)<br>SAP DS 4.2.x |
| UAT | ETL Server | 4 (64 Bit) | 64GB | 1TB | RHEL 7.x (64 Bit)<br>SAP DS 4.2.x |
| Production | ETL Server | 4 (64 Bit) | 64GB | 100GB | RHEL 7.x (64 Bit)<br>SAP DS 4.2.x |
| Production | ETL Server | 4 (64 Bit) | 64GB | 100GB | RHEL 7.x (64 Bit)<br>SAP DS 4.2.x |

| Environment | Server | Cores | Memory | Storage | Software |
|---|---|---|---|---|---|
| Development | Application Server | 8 (64 Bit) | 32GB | 200GB | RHEL 7.x (64 Bit)<br>WebSphere ND 8.5 |
| Development | Batch Server | 8 (64 Bit) | 32GB | 200GB | RHEL 7.x (64 Bit)<br>WebSphere ND 8.5 |
| Development | Audit Database | 4 (64 Bit) | 32GB | 4TB | RHEL 7.x (64 Bit)<br>IBM DB2 LUW 10.5 |
| Development | Application Database | 8 (64 Bit) | 32GB | 12TB | RHEL 7.x (64 Bit)<br>IBM DB2 LUW 10.5 |
| Test | Application Server | 8 (64 Bit) | 32GB | 200GB | RHEL 7.x (64 Bit)<br>WebSphere ND 8.5 |
| Test | Batch Server | 8 (64 Bit) | 32GB | 200GB | RHEL 7.x (64 Bit)<br>WebSphere ND 8.5 |
| Test | Audit Database | 4 (64 Bit) | 32GB | 4TB | RHEL 7.x (64 Bit)<br>IBM DB2 LUW 10.5 |
| Test | Application Database | 8 (64 Bit) | 32GB | 12TB | RHEL 7.x (64 Bit)<br>IBM DB2 LUW 10.5 |
| UAT | Application Server | 8 (64 Bit) | 64GB | 200GB | RHEL 7.x (64 Bit)<br>WebSphere ND 8.5 |
| UAT | Application Server | 8 (64 Bit) | 64GB | 200GB | RHEL 7.x (64 Bit)<br>WebSphere ND 8.5 |
| UAT | Batch Server | 8 (64 Bit) | 64GB | 200GB | RHEL 7.x (64 Bit)<br>WebSphere ND 8.5 |
| UAT | Audit Database | 8 (64 Bit) | 64GB | 4TB | RHEL 7.x (64 Bit)<br>IBM DB2 LUW 10.5 |
| UAT | Application Database | 8 (64 Bit) | 32GB | 12TB | RHEL 7.x (64 Bit)<br>IBM DB2 LUW 10.5 |
| Production | Application Server | 8 (64 Bit) | 64GB | 500GB | RHEL 7.x (64 Bit)<br>WebSphere ND 8.5 |

| Environment | Server | Cores | Memory | Storage | Software |
|---|---|---|---|---|---|
| Production | Application Server | 8 (64 Bit) | 64GB | 500GB | RHEL 7.x (64 Bit)<br>WebSphere ND 8.5 |
| Production | Application Server | 8 (64 Bit) | 64GB | 500GB | RHEL 7.x (64 Bit)<br>WebSphere ND 8.5 |
| Production | Application Server | 8 (64 Bit) | 64GB | 500GB | RHEL 7.x (64 Bit)<br>WebSphere ND 8.5 |
| Production | Batch Server | 8 (64 Bit) | 64GB | 500GB | RHEL 7.x (64 Bit)<br>WebSphere ND 8.5 |
| Production | Audit Database | 8 (64 Bit) | 64GB | 20TB | RHEL 7.x (64 Bit)<br>IBM DB2 LUW 10.5 Enterprise |
| Production | Application Database | 16 (Power7 3.7GHz) | 32GB | 1.2TB | AIX 7.1<br>IBM DB2 LUW 10.5 Enterprise |
| Production | CRM App Server | 8 (64 Bit) | 16GB | 1600GB | Windows Server 2012 R2 Data Center Edition<br>Microsoft CRM 2010 |
| Production | CRM Database | 4 (64 Bit) | 8GB | 1600GB | Windows Server 2012 R2 Data Center Edition<br>MS SQL Server |
| Production | CRM Web Server | 4 (64 Bit) | 4GB | 164GB | Windows Server 2012 R2 Data Center Edition<br>ADX Studio |
| Production | CRM App Server | 8 (64 Bit) | 16GB | 1600GB | Windows Server 2012 R2 Data Center Edition<br>Microsoft CRM 2010 |
| Production | CRM Database | 4 (64 Bit) | 8GB | 1600GB | Windows Server 2012 R2 Data Center Edition<br>MS SQL Server |
| Production | CRM Web Server | 4 (64 Bit) | 4GB | 164GB | Windows Server 2012 R2 Data Center Edition<br>ADX Studio |

| Environment | Server | Cores | Memory | Storage | Software |
|---|---|---|---|---|---|
| Test | CRM App Server | 4 (64 Bit) | 8GB | 164GB | Windows Server 2012 R2 Data Center Edition<br>Microsoft CRM 2010 |
| Test | CRM Database | 4 (64 Bit) | 8GB | 164GB | Windows Server 2012 R2 Data Center Edition<br>MS SQL Server |
| Test | CRM Web Server | 4 (64 Bit) | 4GB | 164GB | Windows Server 2012 R2 Data Center Edition<br>ADX Studio |
| Test | CRM App Server | 4 (64 Bit) | 8GB | 164GB | Windows Server 2012 R2 Data Center Edition<br>Microsoft CRM 2010 |
| Test | CRM Database | 4 (64 Bit) | 8GB | 164GB | Windows Server 2012 R2 Data Center Edition<br>MS SQL Server |
| Test | CRM Web Server | 4 (64 Bit) | 4GB | 164GB | Windows Server 2012 R2 Data Center Edition<br>ADX Studio |
| Development | CRM App Server | 2 (64 Bit) | 4GB | 164GB | Windows Server 2012 R2 Data Center Edition<br>Microsoft CRM 2010<br>ADX Studio |
| Development | CRM Database | 2 (64 Bit) | 4GB | 164GB | Windows Server 2012 R2 Data Center Edition<br>MS SQL Server |
| Training | CRM App Server | 2 (64 Bit) | 4GB | 164GB | Windows Server 2012 R2 Data Center Edition<br>Microsoft CRM 2010 |
| Training | CRM Database | 2 (64 Bit) | 4GB | 164GB | Windows Server 2012 R2 Data Center Edition<br>MS SQL Server |
| Training | CRM Web Server | 2 (64 Bit) | 4GB | 164GB | Windows Server 2012 R2 Data Center Edition<br>ADX Studio |

# THE FLORIDA SENATE

Tallahassee, Florida 32399-1100

**SENATOR ED HOOPER**
16th District

**COMMITTEES:**
Governmental Oversight and Accountability, Chair
Appropriations Subcommittee on Agriculture, Environment, and General Government
Appropriations Subcommittee on Health and Human Services
Health Policy
Infrastructure and Security
Joint Select Committee on Collective Bargaining, Alternating Chair
Joint Administrative Procedures Committee

March 27th, 2019

The Honorable Debbie Mayfield, Chair
Appropriations Subcommittee on Agriculture, Environment, and General Government
201 The Capitol
404 South Monroe Street
Tallahassee, FL 32399-1100

Dear Chair Mayfield:

I am writing to request that Senate Bill 1570, Information Technology Reorganization, be placed on the agenda of the next Appropriations Subcommittee on Agriculture, Environment, and General Government meeting.

Should you have any questions regarding this bill, please do not hesitate to reach out to me. Thank you for your time and consideration.

Warm regards,

Ed Hooper

SENATE APPROPRIATIONS
RECEIVED
19 MAR 27 PM 12:58
SENT TO CHAIRMAN
STAFF DIR. ___ STAFF ___

Cc: Giovanni Betta, Staff Director
Lisa Waddell, Administrative Assistant

REPLY TO:
☐ 3450 East Lake Road, Suite 305, Palm Harbor, Florida 34685-2411 (727) 771-2102
☐ 326 Senate Office Building, 404 South Monroe Street, Tallahassee, Florida 32399-1100 (850) 487-5016

Senate's Website: *www.flsenate.gov*

**BILL GALVANO**
**President of the Senate**

**DAVID SIMMONS**
**President Pro Tempore**

**THE FLORIDA SENATE**

# APPEARANCE RECORD

(Deliver BOTH copies of this form to the Senator or Senate Professional Staff conducting the meeting)

04/16/19
*Meeting Date*

1570
*Bill Number (if applicable)*

Topic Information Technology Reorganization

*Amendment Barcode (if applicable)*

Name David Clark

Job Title Chief of Staff

Address 4050 Esplanade Way
*Street*

Tallahassee FL 32399
*City* *State* *Zip*

Phone 850-922-6535

Email Andrew.Forst@dms.myflorida.co

Speaking: ☑ For ☐ Against ☑ Information

Waive Speaking: ☐ In Support ☐ Against
*(The Chair will read this information into the record.)*

Representing Dept. of Management Services

Appearing at request of Chair: ☐ Yes ☑ No

Lobbyist registered with Legislature: ☑ Yes ☐ No

*While it is a Senate tradition to encourage public testimony, time may not permit all persons wishing to speak to be heard at this meeting. Those who do speak may be asked to limit their remarks so that as many persons as possible can be heard.*

***This form is part of the public record for this meeting.***

S-001 (10/14/14)

**THE FLORIDA SENATE**

# APPEARANCE RECORD

(Deliver BOTH copies of this form to the Senator or Senate Professional Staff conducting the meeting)

4/16/19
*Meeting Date*

1570
*Bill Number (if applicable)*

Topic Information Technology Reorganization

*Amendment Barcode (if applicable)*

Name Carol Bracy

Job Title Consultant

Address 201 E Park Ave, 5th Floor
*Street*

Phone 850-577-0444

Tallahassee FL 32301
*City* *State* *Zip*

Email carol@ballardfl.com

Speaking: ☐ For ☐ Against ☐ Information

Waive Speaking: ☑ In Support ☐ Against
*(The Chair will read this information into the record.)*

Representing Amazon.com

Appearing at request of Chair: ☐ Yes ☑ No

Lobbyist registered with Legislature: ☑ Yes ☐ No

*While it is a Senate tradition to encourage public testimony, time may not permit all persons wishing to speak to be heard at this meeting. Those who do speak may be asked to limit their remarks so that as many persons as possible can be heard.*

***This form is part of the public record for this meeting.***

S-001 (10/14/14)

**THE FLORIDA SENATE**

# APPEARANCE RECORD

(Deliver BOTH copies of this form to the Senator or Senate Professional Staff conducting the meeting)

4-16-19
*Meeting Date*

*Bill Number (if applicable)*

Topic N. W. Florida

*Amendment Barcode (if applicable)*

Name Steve Southerland

Job Title CHAIRMAN

Address 900 KRISTANNA DR.
*Street*

Phone 850-258-9082

PANAMA CITY FL 32405
*City* *State* *Zip*

Email STEVE@SOUTHERLANDFAMILY.COM

Speaking: ☐ For ☐ Against ☑ Information

Waive Speaking: ☐ In Support ☐ Against
*(The Chair will read this information into the record.)*

Representing Stand Up for North Florida

Appearing at request of Chair: ☐ Yes ☒ No

Lobbyist registered with Legislature: ☐ Yes ☒ No

*While it is a Senate tradition to encourage public testimony, time may not permit all persons wishing to speak to be heard at this meeting. Those who do speak may be asked to limit their remarks so that as many persons as possible can be heard.*

***This form is part of the public record for this meeting.***

S-001 (10/14/14)

# CourtSmart Tag Report

**Room:** EL 110 **Case No.:** **Type:**
**Caption:** Senate Appropriations Subcommittee on Agriculture, Environment and General Government **Judge:**

**Started: 4/16/2019 9:01:05 AM**
**Ends: 4/16/2019 9:58:58 AM** **Length: 00:57:54**

**9:01:14 AM** Call to Order
**9:01:16 AM** Sen. Mayfield (Chair)
**9:02:20 AM** S 7098
**9:02:28 AM** Sen. Hooper
**9:04:53 AM** Sen. Berman
**9:05:13 AM** Sen. Hooper
**9:05:42 AM** Sen. Berman
**9:05:52 AM** Sen. Hooper
**9:06:16 AM** Gary Hester, Chief - Government Affairs, Florida Police Chiefs Association (waives in support)
**9:06:27 AM** Matt Butler, Captain, Legislative Affairs/Narcotics, Orange County Sheriff's Office (waives in support)
**9:06:36 AM** Rocco Salvatori, Firefighter, Florida Professional Firefighters (waives in support)
**9:06:52 AM** Sen. Stewart
**9:07:39 AM** Sen. Hooper
**9:09:09 AM** S 1570
**9:09:16 AM** Sen. Hooper
**9:10:56 AM** Sen. Rodriguez
**9:11:14 AM** Sen. Hooper
**9:13:25 AM** Sen. Berman
**9:13:47 AM** Sen. Hooper
**9:14:34 AM** Sen. Berman
**9:14:46 AM** Sen. Hooper
**9:15:15 AM** Sen. Berman
**9:15:37 AM** David Clark, Chief of Staff, Department of Management Services
**9:18:40 AM** Sen. Berman
**9:19:03 AM** D. Clark
**9:21:44 AM** Carol Bracy, Consultant, Amazon.com (waives in support)
**9:21:59 AM** Sen. Hooper
**9:23:03 AM** Tab 3 - Presentation on Environmental Needs of North Florida by Honorable Steve Southerland, Chairman, Stand up for North Florida
**9:23:17 AM** Steve Southerland
**9:45:32 AM** Sen. Broxson
**9:49:52 AM** S. Southerland
**9:55:39 AM** Sen. Mayfield
**9:56:40 AM** Sen. Stewart
**9:57:22 AM** Sen. Mayfield
**9:58:27 AM** Meeting Adjourned