

Agency: 477 Department of Fish and Wildlife
Decision Package Code/Title: AD ISB IT Security Compliance
Budget Period: 2011-13
Budget Level: M2 - Inflation and Other Rate Changes

Recommendation Summary Text:

WDFW requests additional funding to comply with revised IT Security Standards by August 2012 as mandated by the Information Services Board (ISB) Policy 401.S4. WDFW, like many other agencies, operate in the State Governmental Network (SGN) which is a shared network with each agency trusting the other to facilitate the exchange of information and leverage common systems. Many agencies have highly confidential and sensitive personal information regarding the citizens of the state which is a target for identity thieves and other criminals. For the SGN to be effective at securing citizen data in a shared environment, each agency is expected to meet the minimum requirements set forth so to not create loopholes or backdoors for malicious users to use as a method of attacking another agency or the State network as a whole. The following supplemental request is needed to ensure that WDFW is able to meet the minimum requirements of the State IT Security Policy. WDFW is able to achieve only partial compliance within existing resources and additional funding is necessary to meet full requirements in the areas of encrypting confidential data, network access security and event monitoring and logging.

Fiscal Detail

Operating Expenditures	<u>FY 2012</u>	<u>FY 2013</u>	<u>Total</u>
001-1 General Fund - Basic Account-State	70,360	183,160	253,520
104-1 State Wildlife Account-State	105,540	274,740	380,280
Total Cost	175,900	457,900	633,800
 Staffing	 <u>FY 2012</u>	 <u>FY 2013</u>	 <u>Annual Average</u>
FTEs	.7	1.9	1.3

Package Description:

WDFW maintains several unencrypted, unprotected databases containing Washington resident personal information that meet the definition of confidential data. Due to the decentralized nature of the hatchery and wildlife area workforce, nearly 900 WDFW employees connect to the State Government Network (SGN) from many different locations, through multiple internet service providers, utilizing older VPN technology that require only a user id and password pair to verify identity. Event monitoring and logging activities are non-existent, including responding to attempts to compromise the SGN from systems emanating from or targeting Fish and Wildlife systems. This is due to the absence of an organized storage, analysis, and review policy and no available staff resources to perform this work. These current practices do not meet the revised IT Security Standards (Policy 401.S4) set forth by the ISB.

The revised IT Security Standards (Policy 401.S4) provide increased requirements and the expectation that all state agencies achieve full compliance by August 2012. WDFW is able to achieve only partial compliance within existing resources and additional funding is necessary to meet requirements in the areas of encrypting confidential data, network access security and event monitoring and logging.

- Encrypt confidential data: With the requested funding, WDFW will purchase the higher level license necessary to encrypt several databases containing confidential Washington state resident data.

- Network Access security: Additionally, WDFW will switch from the older VPN technology currently used by nearly 900 employees to connect to the SGN to the newly required, two-factor authentication services offered by the Department of Enterprise Services at a monthly, per-user rate.

- Event Monitoring and Logging: WDFW can create event monitoring logs within existing resources. With increased funding, additions to the current Microsoft Enterprise Agreement for capabilities and the additional staff necessary to support and maintain this requirement will be secured.

It is proposed that these changes take effect on or before the August 2012 deadline.

Name and Phone Number of Subject Matter Expert:
Michael DeAngelo, 360-902-2320

Narrative Justification and Impact Statement

What specific performance outcomes does the agency expect?

By encrypting WDFW servers, unauthorized access to confidential information will be prevented reducing the risk of identity theft, loss of public confidence and the potential for legal claims and damages.

Utilizing current VPN technology ensures continued connection to the SGN and safeguards WDFW IT, data and fiscal assets by preventing unauthorized access through two-factor authentication services. A single, unsecure agency can provide "open door" access to the entire SGN.

WDFW agency and employee accountability will increase for all IT system actions, reducing risk that could expose the agency to legal claims and damages.

Performance Measure Detail

Activity: A032 Agency Administration

Incremental Changes

No measures submitted for package

Is this decision package essential to implement a strategy identified in the agency's strategic plan?

This decision package directly relates to the use of sound business practices and effectively managing agency assets as described in Goal 4 of the WDFW 2011-17 Strategic Plan.

Does this decision package provide essential support to one of the Governor's priorities?

This decision package supports the Governor's priorities of providing efficient state government services and providing for the public safety of people and property in Washington state.

Does this decision package make key contributions to statewide results? Would it rate as a high priority in the Priorities of Government process?

This decision package contributes to the statewide result of improving the security of the state IT systems and increased government accountability.

What are the other important connections or impacts related to this proposal?

This decision package supports the overall state direction to become more accountable in protecting state resources from malicious intent and improving securing Washington residents' confidential information from identity theft and other crimes.

What alternatives were explored by the agency, and why was this alternative chosen?

The Department explored ways of implementing services internally to lower the implementation costs. In particular, the 2-factor authentication requirement, because it is the most costly component of the package. In the end, rather than building an internal service at a lower cost, it was decided that leveraging DIS services was more consistent with the direction of the state and can further help the state achieve greater economies of scale.

What are the consequences of not funding this package?

Without sufficient funding of this package, WDFW will not be in compliance with the state security standard by August 2012 as required. In addition, the continued lack of protection of state resources and resident personal information will increase financial and legal risk as well as reduce confidence in the state's ability to manage its technology resources.

What is the relationship, if any, to the state's capital budget?

None.

What changes would be required to existing statutes, rules, or contracts, in order to implement the change?

None.

Expenditure and revenue calculations and assumptions

Event Monitoring and Logging (software and storage):

- Microsoft System Center Suite training and configuration added to current MS enterprise agreement: \$910 per biennium.
- One FTE (at the ITS 4 level) starting 4/1/2012 to perform activities of configuration, administration, reviewing and responding to log events: \$115,500 (\$184,800 for future biennia).

Network Access Security:

- VPN (DIS Shared service) at \$17.50/user/month for 900 users, assuming a 4/1/2012 start date: \$236,250 (\$378,000 for future biennia).

Encrypt confidential data:

- Upgrade database software: \$68,880 (\$17,220/processor/year x 2 processors).
- Expand virtual server environment to support database servers and storage: \$23,890. \$1,526/month lease beginning 4/1/2012 plus one-time setup fee of \$1,000 (\$36,624 for future biennia).
- Backup services (DIS Shared service) to encrypt confidential data: \$60,000. (Note: the actual cost is \$140,000 per biennium, but we will achieve \$80,000 per biennium savings when we shut down our in-house backup service).

Administrative overhead is calculated at 23.51% and included in Object E. Total administrative overhead is \$33,500 in FY12 and \$87,200 in FY13 and ongoing. Administrative FTE's are included at .40 in FY12 and .90 in FY13 and ongoing.

Which costs and functions are one-time? Which are ongoing? What are the budget impacts in future biennia?

One-time costs:

- One-time setup fee for leased server: \$1,000.

Ongoing costs:

- All other costs: \$632,800.

Impacts to future biennia:

- Salary, benefits, leases and services purchased from DIS assume a start date of 4/1/2012. Impacts to future biennia total \$457,900 per year. Administrative overhead of \$87,200 per year is included in this figure.

<u>Object Detail</u>	<u>FY 2012</u>	<u>FY 2013</u>	<u>Total</u>
A Salaries And Wages	17,300	69,300	86,600
B Employee Benefits	5,800	23,100	28,900
E Goods And Services	152,800	365,500	518,300
Total Objects	175,900	457,900	633,800