

Administrative and Supporting Services

110 - PL - WC - ENTERPRISE IT SECURITY

Agency Submittal: 11-2017-19-YR Agency Req

Budget Period: 2017-19

SUMMARY

Of the 11 million patient records compromised in the U.S. in June 2016, 41.4 percent of reported breach incidents involved hacking, 41.4 percent involved insider wrongdoing/error, and 17.2 percent involved theft/loss of devices or paper records. The key to thwarting this data loss, whether externally or internally driven, is visibility and containment. This request is for \$5,843,000 (\$4,791,000 GF-State) and 6.0 FTEs to protect sensitive client data.

PROBLEM STATEMENT

DSHS is required by state and federal law to protect and maintain the privacy and security of sensitive client information. This includes Social Security Numbers (SSN), medical and psychiatric data, names and locations of clients, etc. Security attacks are becoming increasingly complex, making the discovery, prevention, and immediate response to unauthorized access to client data essential. The longer it takes to detect a breach (dwell time), the more costly it becomes to resolve. An attacker is only as good as their ability to move throughout a network and access sensitive areas.

Increased Costs - Delays in Detecting a Data Breach

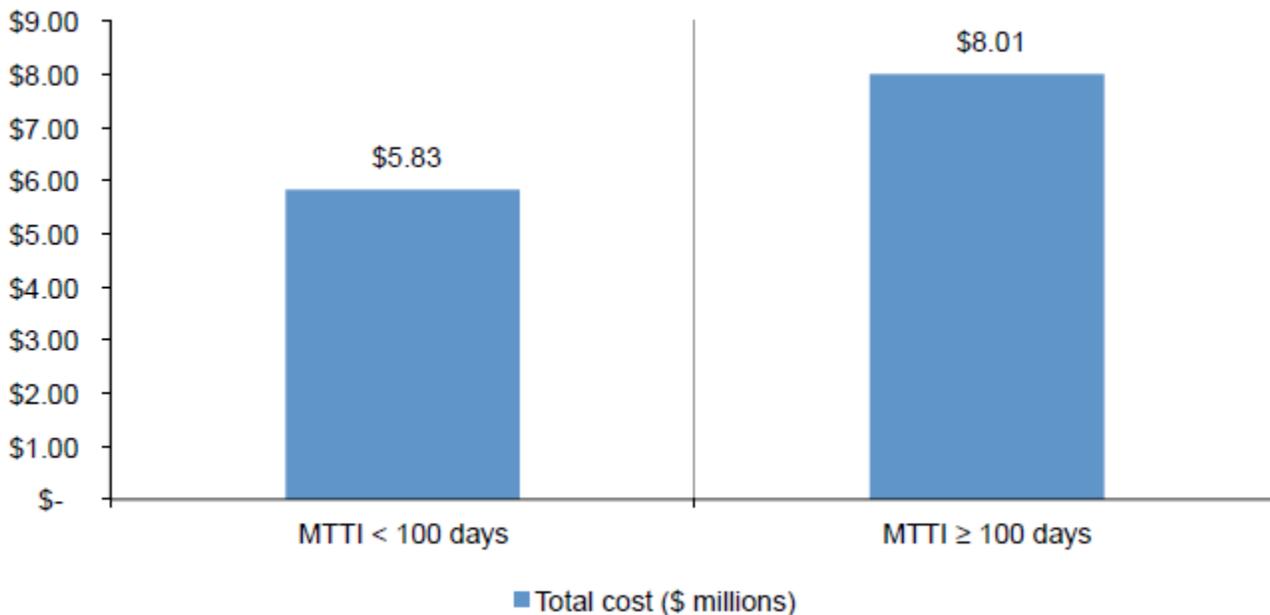


Figure 1-Mean time to identify the breach event (MTTI) Source: Ponemon Institute (June 2016)



DSHS VISION
 People are healthy • People are safe • People are supported • Taxpayer resources are guarded

DSHS MISSION
 To transform lives

DSHS VALUES
 Honesty and Integrity • Pursuit of Excellence • Open Communication • Diversity and Inclusion • Commitment to Service

PROPOSED SOLUTION

ITEM	ESTIMATED COST (FISCAL YEARS 2018-2019 TOTAL FUNDS)	
PLAN/DESIGN HYBRID SECURITY OPERATIONS CENTER (SOC) (REQUEST FOR PROPOSAL -RFP)		\$1,000,000
IMPLEMENTATION		\$3,157,000
6 FTES	\$136,333/YEAR	\$1,636,000
TRAINING		\$ 50,000
	Total	\$5,843,000 Total Funds

Operationalizing – Funding this request allows DSHS’s Services and Enterprise Support to implement the Security Operations Center (SOC), which will provide the tools and expertise to prevent data breaches, fines, and litigation. The SOC will utilize a hybrid model which includes a combination of on premise personnel and tools, as well as Software as a Service (SaaS) contract. On premise, the SOC will maximize DSHS’s current use of the WaTech security information and event management solution by adding the necessary logging archiver mandated by federal and state data retention laws. The SOC will also improve database, application, and mobile application security, and provide employees and contractors a means to communicate with clients utilizing secure mobile messaging. Taking advantage of Software as a Service (SaaS), the SOC will introduce an Enterprise Immune System that provides real-time threat protection from evolving cyber threats. Additionally, the SOC will implement Incident Response software to tie together response and reporting throughout the eight individual DSHS Administrations, the DSHS Information Security Office, and the WaTech Security Operations Center. This will streamline workflows and provide trend and analysis reporting and a documentation store for regulators. Finally, with an aim toward becoming an “employer of choice” and recognizing the need to treat data security as a continuous enterprise-wide process, DSHS must offer its security analysts additional training as the threats to data security evolve.

Personnel – The DSHS Information Security Office requires two additional FTEs: one Information Technology Systems/Application Specialist 6 (IT/AS6) for contracts security, and one IT/AS6 for Cloud security. Contracts security, particularly for those contracts with data share agreements, requires increasing privacy and data security scrutiny. While the standard Data Sharing Requirements Exhibit in use at DSHS affords a baseline for security considerations, more often than not, a vendor agreement still requires a review, particularly for smaller-sized and individual vendors. Given the volume of contacts entered into by DSHS, this focused review and selection of controls tailored to each contract consumes a significant amount of analyst resources, which are currently at capacity. Regarding Cloud security, the legal and technical complexity of the DSHS implementation of Azure/O365 requires the addition of personnel resources. Cloud security architecture and identity management are emerging skills and the current resource is at capacity.

One IT/AS6 Security Analyst is required by the DSHS Rehabilitation Administration (RA), which includes the Division of Vocational Rehabilitation, Juvenile Rehabilitation, the Office of Juvenile Justice, and the Special Commitment Center. RA has no dedicated Information Technology (IT) Security Administrator at the administration level and only the Division of Vocational Rehabilitation has a FTE dedicated to this role. With DSHS’ increased commitment to proactive privacy and security measures has come an increased workload to coordinate, manage and maintain compliance with federal and state requirements. Currently, this increase workload, in addition to regular duties, is divided among existing staff in

110 - PL - WC - Enterprise IT Security

Juvenile Rehabilitation and the Special Commitment Center. A dedicated FTE to specialize in the area of IT security would allow the administration to assume a much more proactive IT security posture, as well as provide a critical resource to detect, report and react to security incidents.

Two IT/AS6 positions are required for the Behavioral Health Administration (BHA), which consists of the Division of Behavioral Health and Recovery, Western State Hospital, Eastern State Hospital, and the Child Study and Treatment Center. BHA does not have resources dedicated to data security. The volume and complexity of its sensitive data, combined with the drive for electronic health records necessitates these FTEs.

One IT/AS6 Security Analyst is required in the Technology Services Division within the Services and Enterprise Support Administration. The Technology Services Division is responsible for maintaining the operational security for agency-wide information technology services such as network infrastructure, shared messaging, telephone and voice services, Internet/Intranet services and enterprise architecture.

EXPECTED RESULTS

In Governor Directive 16-01, Governor Inslee defined critical systems as those used for public safety, public health, accounting/financial administration, state revenue collection, and the administration of services for the vulnerable and/or disadvantaged. DSHS provides these critical services to residents within the state.

By funding this request, eligible clients throughout the state will have access to global cyber security threat intelligence, and highly skilled security intelligence analysts as a normal extension of DSHS resources. DSHS's valued clients can access services and trust that their sensitive data (such as SSN, payment information, substance abuse and mental health information, and other protected health information) is afforded protection from:

- Inadvertent misuse by an insider
- External attacks such as ransomware
- Abuse by a malicious insider

If this request is not funded, sensitive client data within critical systems as defined by Governor Inslee is at risk for potential loss and exploitation, increasing DSHS exposure for fines and litigation.

DSHS clients eligible for services are some of the most vulnerable in our society. By funding this request, the state is demonstrating real commitment to protect their data.

STAKEHOLDER IMPACT

It is anticipated that the Legislature, employee unions, and the Department of Labor and Industries will all favorably endorse DSHS's expanded efforts to concentrate qualified, professional expertise at the critical issue of safety, security and occupational health.

Agency Contact: Don Petrich, (360) 902-7831

Program Contact: Kim Anderson, (360) 902-8443

OTHER CONNECTIONS

Performance Outcomes/Important Connections

1. Does this DP provide essential support to one or more of the Governor's Results Washington priorities?

Goal 5: Efficient, Effective & Accountable Government - Customer Satisfaction and Confidence - 1.1 Increase customer services.

2. The decision package meets the following DSHS' strategic objectives:

ET and RDA 5.9: Protect sensitive client data.

ET/TSD 5.14: Pursue excellence in the technology services we offer.

3. Identify other important connections or impacts below. (Indicate 'Yes' or 'No'. If 'Yes' identify the connections or impacts related to the proposal.)

- a) Regional/County impacts? Yes
- b) Other local government impacts? Yes
- c) Tribal government impacts? No
- d) Other state agency impacts? Yes
- e) Responds to specific task force, report, mandate or executive order? Yes
- f) Does request contain a compensation change or require changes to a Collective Bargaining Agreement? No
- g) Facility/workplace needs or impacts? No
- h) Capital budget impacts? Yes
- i) Is change required to existing statutes, rules or contracts? No
- j) Is the request related to litigation? Yes
- k) Is the request related to Puget Sound recovery? No
- l) Other important connections? Yes

4. Please provide a detailed discussion of connections/impacts identified above.

Implementation of the system will improve database security, application security, mobile application security, and provide employees and contractors a means to communicate with clients utilizing secure mobile messaging. Eligible clients throughout the state will have access to global cyber security threat intelligence, and highly skilled security intelligence analysts as a normal extension of DSHS resources. Our valued clients can access DSHS services and trust that their sensitive data is protected from user mistakes and malicious attacks.

110 - PL - WC - Enterprise IT Security

Alternatives/Consequences/Other

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

- a. Do nothing. DSHS non-compliance with federal and state data protection mandates creates risk of tort liability and potentially exposes sensitive data of DSHS clients.
- b. DSHS considered an in-house, fully staffed Security Operations Center with response capabilities 24 hours a day, seven days a week. The planning, design, building and ongoing maintenance and operational costs of this solution are cost prohibitive. Further, the minimum number of additional FTEs required for staffing the operations center is nine, even if DSHS trained other staff to triage potential incidents for after-hours and weekend support, in addition to those identified as critically necessary above. Moreover, the highly specialized skillset required for these nine FTEs, when available, has an extremely high burnout rate, leaving DSHS vulnerable to a gap in critical operational expertise.

6. How has or can the agency address the issue or need within its current appropriation level?

DSHS, as is common in government and private sector, has been operating under a traditional model of securing its network perimeter, orienting its resources around suspicious activity, determining a course of action based on limited holistic information, and executing a canned response based on limited knowledge. There are two major business challenges that necessitate a change of course: Bring Your Own Device (BYOD), and “the Cloud.” To maintain a client-centered approach to delivering services, DSHS recognizes the need for mobile applications and Cloud adoption. Our current appropriation level does not afford the level of security necessary for privacy and data protection that keeps pace with technology.

7. Does this decision package include funding for any IT-related costs (hardware, software, services, cloud-based services, contracts or IT staff)?

- No
- Yes (Include an IT Addendum)

Fiscal Detail**110 - PL - WC - Enterprise IT Security**

Operating Expenditures	<u>FY 2018</u>	<u>FY 2019</u>	<u>FY 2020</u>	<u>FY 2021</u>
001-1 General Fund-State	3,470,000	1,321,000	1,321,000	1,321,000
001-2 General Fund-Federal	762,000	290,000	290,000	290,000
Total Cost	4,232,000	1,611,000	1,611,000	1,611,000
Staffing	<u>FY 2018</u>	<u>FY 2019</u>	<u>FY 2020</u>	<u>FY 2021</u>
FTEs	6.0	6.0	6.0	6.0

Performance Measure Detail

Activity:	Incremental Changes			
	<u>FY 2018</u>	<u>FY 2019</u>	<u>FY 2020</u>	<u>FY 2021</u>
Program: 110				
K001 Administration and Supporting Services	0	0	0	0
No measures submitted for package				

Object Detail

	<u>FY 2018</u>	<u>FY 2019</u>	<u>FY 2020</u>	<u>FY 2021</u>
A Salaries and Wages	562,000	562,000	562,000	562,000
B Employee Benefits	178,000	178,000	178,000	178,000
EG Employee Professional Development and Training	25,000	25,000	25,000	25,000
EN Personnel Services	38,000	38,000	38,000	38,000
EY Software Licenses, Maintenance, and Subscription-Based C	238,000	238,000	238,000	238,000
EZ Other Goods and Services	3,135,000	550,000	550,000	550,000
G Travel	2,000	2,000	2,000	2,000
J Capital Outlays	36,000	0	0	0
TZ Intra-agency Reimbursements	18,000	18,000	18,000	18,000
Total Objects	4,232,000	1,611,000	1,611,000	1,611,000

DSHS Source Detail**Overall Funding**

Operating Expenditures	<u>FY 2018</u>	<u>FY 2019</u>	<u>FY 2020</u>	<u>FY 2021</u>
-------------------------------	-----------------------	-----------------------	-----------------------	-----------------------

Fund 001-1, General Fund-State**Sources Title**

0011 General Fund State	3,470,000	1,321,000	1,321,000	1,321,000
-------------------------	-----------	-----------	-----------	-----------

Total for Fund 001-1 **3,470,000** **1,321,000** **1,321,000** **1,321,000**

Fund 001-2, General Fund-Federal**Sources Title**

FLIV Fed Entered as Lidded (various%)	762,000	290,000	290,000	290,000
---------------------------------------	---------	---------	---------	---------

Total for Fund 001-2 **762,000** **290,000** **290,000** **290,000**

Total Overall Funding **4,232,000** **1,611,000** **1,611,000** **1,611,000**

Information Technology Addendum

Recsum Code and Title 110-PL-WC-Enterprise IT Security

Part 1: Itemized IT Costs

Please itemize any IT-related costs, including hardware, software, services (including cloud-based services), contracts (including professional services, quality assurance, and independent verification and validation) or IT staff. Be as specific as you can. (See Chapter 12.1 of the OFM Operating Budget Instructions for guidance on what counts as “IT-related costs.”)

Information Technology Items in this DP (insert rows as required)	FY 2018	FY 2019	FY 2020	FY 2021
Plan & Design Hybrid SOC (RFP)	1,000,000	0	0	0
Log Archiver (est WaTech)	550,000	25,000	25,000	25,000
Application Scanner (term license)	238,000	238,000	238,000	238,000
Database Scanner (support)	19,000	19,000	19,000	19,000
Secure Text Solution (est)	550,000	20,000	20,000	20,000
Enterprise Immune System – Realtime Threat Protection (Hardware, Software, and Services)	264,000	264,000	264,000	264,000
Encryption Key Management Solution (service, est)	200,000	200,000	200,000	200,000
Incident Response Software (est)	550,000	20,000	20,000	20,000
IT/AS6 FTEs (6)	836,000	800,000	800,000	800,000
Security training quote by Stormwind	25,000	25,000	25,000	25,000
Total Cost	4,232,000	1,611,000	1,611,000	1,611,000

Note: The following are vendor estimates as vendors were unwilling to provide official quotes without commitment from DSHS:

- Plan & Design Hybrid SOC (RFP)
- Log Archiver (est, WaTech)
- Application Scanner (term license)
- Database Scanner (support)
- Secure Text Solution (est)
- Enterprise Immune System – Real-time Threat Protection (Hardware, Software, and Services)
- Encryption Key Management Solution (service, est)

Part 2: Identify IT Projects

1. Does this decision package fund the development or acquisition of a new or enhanced software or hardware system or service? (Yes)
2. Does this decision package fund the acquisition or enhancements of any agency data centers? (See OCIO Policy 184 for definition.) (No)
3. Does this decision package fund the continuation of a project that is, or will be, under OCIO oversight? (See OCIO Policy 121.) (No)

If you answered “yes” to any of these questions, you must complete a concept review with the OCIO before submitting your budget request. Refer to Chapter 12.2 of the Operating Budget Instructions for more information.