Washington State
Department of Social
& Health Services

AERA Administrative and
External Relations Administration

FINAL

2014 SUPPLEMENTAL BUDGET

INFORMATION SECURITY PROGRAM IMPROVEMENTS

Request	FY14	FY15	13-15
FTE	0.0	0.0	0.0
GF-State	$898,000	$1,659,000	$2,557,000
Total	**$1,095,000**	**$2,023,000**	**$3,118,000**

DECISION PACKAGE SUMMARY

The Information System Services Division (ISSD) requests FTEs, contracts, and tools in order to address critical security program updates and controls in light of increasingly urgent cyber security threats. ISSD is the administrative home for the Department of Social and Health Services (DSHS) Information Technology (IT) Security program. Funding this request will allow DSHS to be positioned to improve the overall agency information security posture in response to evolving needs and support compliance to current and future regulatory and Office of the Chief Information Officer (OCIO) policies.

PROBLEM STATEMENT

The Information Security program within the Department of Social and Health Services requires improvement to keep pace with changing technologies, increased cyber security threats, and industry best practice. There are a limited number of well-trained Information Security staff within the Department and no consistent toolset used to review and monitor compliance. The requested resources compliment investments underway at Consolidated Technology Services (CTS) and will use the new CTS security service offerings once available. While the OCIO's office is responsible for the state's overall IT Security program, each agency is responsible for administering their agency program within these parameters. The IT security staff will work closely with the OCIO on policy and program monitoring within DSHS.

PROPOSED SOLUTION

This funding request will provide:
1. Necessary support for the agency security improvement strategy with increased number of trained and dedicated IT Security resources to support the agency-wide program:
   a. Two FTEs at an Information Technology Specialist (ITS) 4 level and one FTE at an ITS 5 level to support and improve monitoring of the central agency IT Security program.
   b. Six FTEs at ITS 6 level to provide dedicated trained Security resources within the Administrations and ISSD to provide program specific support and act as 'first responders' in the event of security incidents. These FTEs would be housed within ISSD and report to the DSHS Security Officer. Relevant core IT security training would be

provided to these FTEs to establish a consistent best practices foundation. Funding would be provided to program 110 to pay for the positions. This will move DSHS toward a more centralized and consistent posture for the overall DSHS Security Program.

    (1) The six positions would be apportioned as follows:

        (a) Two FTEs within ISSD to provide security administration for centrally managed applications as well as core network and other centrally managed infrastructure.

        (b) One FTE each for Economic Services Administration (ESA), Juvenile Justice and Rehabilitation Administration (JJRA), Children's Administration (CA) and Aging and Long-Term Support Administration (ALTSA).

2. Security tools (software) to address existing program review/assessment gaps. A significant focus is the maturation of a Vulnerability Management program. This investment will support implementation of one or more standard tools that can be widely used within DSHS.

3. Contracted IT Security resources to augment state staff. These contract resources will assist in rapidly building the missing security program elements, establishing a stronger posture, providing project assistance and transferring skills and abilities to staff members.

EXPECTED RESULTS

1. Improved Information Security program best practice posture that can be measured by improved overall maturity scores on the NIST 800-53 Security Framework.

2. There will be more consistent and predictable control of information security risks and an overall improvement in risk management across DSHS.

3. Establishment of a Vulnerability Management program that will proactively identify security vulnerabilities across infrastructure and applications so remediation can be accomplished to continually identify and remediate risks.

4. An overall improved alignment and compliance with regulatory requirements and OCIO policies and standards.

This request supports Results Washington Goal to ensure efficiency, performance, and accountability to the public by providing transparency and accountability in state agency operations.

STAKEHOLDER IMPACT

Improvements to the program benefit citizens, business partners, and government partners with improved safeguards for data and systems.