

2017-19 Biennium Budget Decision Package

Agency: 163 - Consolidated Technology Services (WaTech)

Decision Package Code/Title: A9 - Enterprise Security

Budget Period: 2017-19

Budget Level: PL – Performance Level

Agency Recommendation Summary Text:

Consolidated Technology Services (WaTech) requests \$5,882,000 in the 2017-19 Biennium to support the creation of the new Office of Cyber Security (OCS) while still maintaining crucial infrastructure security services delivered by WaTech to protect agencies' critical data. This package proposes adjustments to the Enterprise Security Infrastructure allocation while creating a new statewide Cybersecurity allocation to support that line of services.

Fiscal Summary:

| Operating Expenditures | FY 2018 | FY 2019 | FY 2020 | FY 2021 |
|------------------------|------------------|------------------|------------------|------------------|
| Fund 458-6 | 2,941,000 | 2,941,000 | 2,941,000 | 2,941,000 |
| Total Cost | 2,941,000 | 2,941,000 | 2,941,000 | 2,941,000 |
| Staffing | FY 2018 | FY 2019 | FY 2020 | FY 2021 |
| FTEs | 0 | 0 | 0 | 0 |
| Revenue | FY 2018 | FY 2019 | FY 2020 | FY 2021 |
| Fund 458-6 | 2,941,000 | 2,941,000 | 2,941,000 | 2,941,000 |
| Object of Expenditure | FY 2018 | FY 2019 | FY 2020 | FY 2021 |
| Obj. A | 809,000 | 809,000 | 809,000 | 809,000 |
| Obj. B | 252,000 | 252,000 | 252,000 | 252,000 |
| Obj. E | 1,141,000 | 1,141,000 | 1,141,000 | 1,141,000 |
| Obj. G | 20,000 | 20,000 | 20,000 | 20,000 |
| Obj. J | 284,000 | 284,000 | 284,000 | 284,000 |
| Obj. T | 435,000 | 435,000 | 435,000 | 435,000 |

Package Description

Information security applies to the protection of information across the state's networks and the access to applications, software and, data that reside in agency data centers, the State Data Center, and the Quincy Data Center. This requires dedicated equipment and software for monitoring traffic and inspecting data. WaTech is also required to set standards and policy direction for state government. There are many state and federal regulations related to information security that apply to the data kept and maintained by state government.

These statewide security services are funded through the Enterprise Security Infrastructure allocation, which totaled \$16,525,000 in 2015-17. However, of this amount \$3,240,000 was designated for disaster recovery, leaving \$13,285,000 – or approximately \$6.6 million each year for ongoing security activities.

OCS shares the Enterprise Security Infrastructure allocation with the WaTech Information Security Office's section that manages infrastructure security, known as Security Infrastructure Services (SIS). This unit maintains the managed firewalls and other key services such as vulnerability assessment, logging and monitoring, and domain naming.

Office of Cyber Security (OCS)

The OCS is responsible for establishing and leading the strategic direction of cyber security for Washington State by providing policy and technology leadership for state government. It is organized into teams that divide the responsibilities of protecting the state's infrastructure from cyber threats.

- Cybersecurity Communications Integration Center (WA-CCIC) is the center for information sharing and monitoring of enterprise security. It monitors and manages all aspects of enterprise security in near real-time from a single, centralized location. It discovers and prioritizes events gathered from multiple systems and devices, and uses this information to proactively mitigate security incidents before they happen, or minimize damage before business operations become compromised.
- Computer Emergency Readiness Team (WA-CERT) performs and facilitates incident-handling when responding to an agency or statewide cybersecurity events.
- Information Sharing and Analysis Center (WA-ISAC) promotes the development, understanding, and awareness of actionable intelligence and analysis. Their core mission is similar is to improve the overall cybersecurity posture of the state through collaboration and information-sharing among public and private sector partners.
- State Information Security Program (WA-SISP) provides expertise in the deployment of industry-leading best practices and technologies statewide to agencies, boards, and commissions, enabling the secure delivery of government services to citizens and businesses
- Security Policy and Compliance (WA-SPC) helps agencies reduce risk in architecture, network design, and application integrity by ensuring agencies follow the state-approved security architecture and security policies.

Security Infrastructure Services (SIS)

WaTech Security Infrastructure Services (SIS) maintains the enterprise infrastructure that protects the Washington State computer network from cyber threats such as hackers and viruses. All agencies on the State Government Network (SGN) and the Intergovernmental Network (IGN) can rely on a safe network environment. The core services are:

- Managed firewalls are designed to protect the state network from unauthorized access and malicious attacks.
- Vulnerability assessment, which is a proactive process agencies use to protect network assets by identifying and tracking system and application vulnerabilities, and being able to take preventative actions before an exploit occurs.
- Logging and monitoring service provides monitoring of all system logs generated by network infrastructure and security equipment to centralize the visibility and report/alert on abnormal traffic detection in near real time allowing agencies to take preventative actions.

Security infrastructure has to grow to accommodate increases in network capacity and utilization, and the demands on this unit have grown significantly over the years, attributed to adding new

agencies to the managed firewall service and supporting disaster recovery with remote firewalls in Philadelphia and Boulder Colorado. There were 75 managed firewalls in FY 2014, increasing to 99 in FY 2015, and 103 in FY 2016. The number of agencies receiving vulnerability assessment services similarly grew, with 12 agencies in FY 2014, 16 in FY 2015, and 22 in FY 2016. All this was accomplished without increasing the staff dedicated to these services.

The cost of maintaining these critical services totals \$19,167,236 for the biennium (\$11,407,965 for OCS and \$7,759,271 for SIS), which exceeds the Enterprise Security Infrastructure allocation by \$5,882,236. Therefore WaTech is requesting \$5,882,000 additional revenue and spending authority. Also, WaTech proposes the creation of a new Cybersecurity allocation to cover the activities of the OCS, and a reduction of the Enterprise Security Infrastructure allocation from \$13,285,000 to \$7,759,000 to cover the costs of enterprise security services managed by SIS.

Base Budget: If the proposal is an expansion or alteration of a current program or service, provide information on the resources now devoted to the program or service.

There is not a fund source specific to the OCS. OCS shares the statewide Enterprise Security Infrastructure allocation with the SIS that manages infrastructure security – primarily firewalls, but also other core services such as domain naming, logging and monitoring, and vulnerability assessment. The expansion of OCS occurred in the second half of FY 2016. Expenditures in that year totaled \$1.9 million, but for the first six months of the year only four staff were designated as Cybersecurity, and it was only after January 2016 that it grew to the 20 staff assigned to the new office.

Decision Package expenditure, FTE and revenue assumptions, calculations and details:

Please see attached backup.

Decision Package Justification and Impacts

What specific performance outcomes does the agency expect?

The budget request supports the WaTech strategic roadmap for new and enhanced security capabilities.

Performance Measure detail:

The decision package supports the Results Washington goal #5: Efficient, Effective and Accountable Government. Threat prevention technology and standards support the goal of being accountable with the state's data resources.

Fully describe and quantify expected impacts on state residents and specific populations served.

State government maintains vast amounts of sensitive data on millions of Washington State citizens that need to be protected. If accessed by unauthorized users, not only can agency operations can be disrupted, but the personal information of citizens using those services will be at risk.

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

| Impact(s) To: | | Identify / Explanation |
|----------------------------|----|------------------------|
| Regional/County impacts? | No | Identify: |
| Other local gov't impacts? | No | Identify: |

| | | |
|---|-----|--|
| Tribal gov't impacts? | No | Identify: |
| Other state agency impacts? | Yes | Identify: State agencies within these allocations and the state's citizens whose private data must be protected. |
| Responds to specific task force, report, mandate or exec order? | No | Identify: |
| Does request contain a compensation change? | No | Identify: |
| Does request require a change to a collective bargaining agreement? | No | Identify: |
| Facility/workplace needs or impacts? | No | Identify: |
| Capital Budget Impacts? | No | Identify: |
| Is change required to existing statutes, rules or contracts? | No | Identify: |
| Is the request related to or a result of litigation? | No | Identify lawsuit (please consult with Attorney General's Office): |
| Is the request related to Puget Sound recovery? | No | If yes, see budget instructions Section 14.4 for additional instructions |

Identify other important connections

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

Agencies maintain data that if accessed by unauthorized users can disrupt state operations, and risk the private personal information of the citizens using those services. Social and health agencies (e.g. DSHS, Department of Health) retain highly sensitive private health information, while agencies such as Employment Security or L&I have employment data or Social Security Numbers that could be exploited if accessed.

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

WaTech can maintain its present level of security monitoring and response, and has been effective at doing so, but as new threats emerge the state may not have the capacity to respond promptly and appropriately.

What are the consequences of not funding this request?

Not funding this request will entail delivering enterprise services to agencies on a first-come first-served basis, with resulting backlogs or inability to respond to agencies' requests for new services or support of existing services. It exposes the state to the risk of future cybersecurity breaches that it will not be able to respond to.

How has or can the agency address the issue or need in its current appropriation level?

Similar to a previous question, WaTech can maintain its present level of security monitoring and response, but may not have the capacity to respond to new threats as necessary.

Other supporting materials:

Please see attached backup.

Information technology: Does this Decision Package include funding for any IT-related costs, including hardware, software, services (including cloud-based services), contracts or IT staff?

No 

Yes Continue to IT Addendum below and follow the directions on the bottom of the addendum to meet requirements for OCIO review.)

2017-19 IT Addendum

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 operating budget instructions for guidance on what counts as “IT-related costs”)

| Information Technology Items in this DP <i>(insert rows as required)</i> | FY 2018 | FY 2019 | FY 2020 | FY 2021 |
|---|------------------|------------------|------------------|------------------|
| Software and licensing | 1,141,000 | 1,141,000 | 1,141,000 | 1,141,000 |
| Equipment | 284,000 | 284,000 | 284,000 | 284,000 |
| Staff | 1,081,000 | 1,081,000 | 1,081,000 | 1,081,000 |
| Internal agency costs | 435,000 | 435,000 | 435,000 | 435,000 |
| Total Cost | 2,941,000 | 2,941,000 | 2,941,000 | 2,941,000 |

Part 2: Identifying IT Projects

If the investment proposed in the decision package is the development or acquisition of an IT project/system, or is an enhancement to or modification of an existing IT project/system, it will also be reviewed and ranked by the OCIO as required by RCW 43.88.092. The answers to the three questions below will help OFM and the OCIO determine whether this decision package is, or enhances/modifies, an IT project:

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

Step A7 - Enterprise Security

| Expenditures | FY 2018 | FY 2019 | Biennium 2017-19 |
|--------------|---------------------|---------------------|---------------------|
| FTE | - | - | - |
| Object A | \$ 808,658 | \$ 808,658 | \$ 1,617,316 |
| Object B | \$ 251,756 | \$ 251,756 | \$ 503,512 |
| Object E | \$ 1,141,031 | \$ 1,141,031 | \$ 2,282,062 |
| Object G | \$ 20,293 | \$ 20,293 | \$ 40,587 |
| Object J | \$ 283,902 | \$ 283,902 | \$ 567,804 |
| Object T | \$ 435,477 | \$ 435,477 | \$ 870,954 |
| Total | \$ 2,941,118 | \$ 2,941,118 | \$ 5,882,236 |

| Revenue | FY 2018 | FY 2019 | Biennium 2017-19 |
|----------|--------------|--------------|------------------|
| Fund 458 | \$ 2,941,118 | \$ 2,941,118 | \$ 5,882,236 |

| | FY 2018 | FY 2019 | Biennium 2017-19 |
|------------------------|----------------|----------------|------------------|
| Revenue | \$ 6,642,500 | \$ 6,642,500 | \$ 13,285,000 |
| Expenditures | \$ 9,583,618 | \$ 9,583,618 | \$ 19,167,236 |
| Difference (shortfall) | \$ (2,941,118) | \$ (2,941,118) | \$ (5,882,236) |

Revenue

Security Infrastructure 2015-17

| | |
|-----------------------|----------------------|
| Biennial Total | \$ 16,525,000 |
| Disaster Recovery (-) | \$ (3,240,000) |
| | <u>\$ 13,285,000</u> |
| Annual Revenue | \$ 6,642,500 |

Expenditures

| Security Infrastructure Services (SIS) | | | |
|--|---------------------|---------------------|---------------------|
| Expenditures | FY 2018 | FY 2019 | Biennium 2017-19 |
| FTE | 6.8 | 6.8 | 6.8 |
| A -Salaries | \$ 496,477 | \$ 496,477 | \$ 992,955 |
| B- Benefits | \$ 163,454 | \$ 163,454 | \$ 326,908 |
| E - Goods and Services | \$ 1,508,067 | \$ 1,508,067 | \$ 3,016,135 |
| E - Internal Purchases | \$ 454,449 | \$ 454,449 | \$ 908,898 |
| G - Travel | \$ 2,126 | \$ 2,126 | \$ 4,251 |
| J - Capital | \$ 925,093 | \$ 925,093 | \$ 1,850,186 |
| P - Debt | \$ 97,769 | \$ 97,769 | \$ 195,538 |
| T- Transfers | \$ 232,200 | \$ 232,200 | \$ 464,400 |
| Total | \$ 3,879,636 | \$ 3,879,636 | \$ 7,759,271 |

Note: Based on FY 2016

Includes service desk (3409) chargeback

| Office of Cyber Security (OCS) | | | |
|--------------------------------|---------------------|---------------------|----------------------|
| Expenditures | FY 2018 | FY 2019 | Biennium 2017-19 |
| FTE | 23.0 | 23.0 | 23.0 |
| A -Salaries | \$ 2,138,531 | \$ 2,138,531 | \$ 4,277,063 |
| B- Benefits | \$ 656,892 | \$ 656,892 | \$ 1,313,785 |
| E - Goods and Services | \$ 1,606,000 | \$ 1,606,000 | \$ 3,211,999 |
| E - Internal Purchases | \$ 51,759 | \$ 51,759 | \$ 103,518 |
| G - Travel | \$ 64,000 | \$ 64,000 | \$ 128,000 |
| J - Capital | \$ - | \$ - | \$ - |
| P - Debt | \$ - | \$ - | \$ - |
| T- Transfers | \$ 1,186,800 | \$ 1,186,800 | \$ 2,373,600 |
| Total | \$ 5,703,982 | \$ 5,703,982 | \$ 11,407,965 |

Ramos, Deborah (WaTech)

From: Lee, Larry (WaTech)
Sent: Monday, August 29, 2016 8:15 AM
To: Fitzgerald, Judy (WaTech); Kirk, Agnes (OCS)
Subject: WaTech DP Consult for SR1608_04324 - WaTech - PL A9 Enterprise Security

Good morning Judy and Agnes,

This email is to summarize your Decision Package (DP) Consultation with WaTech. Your Service Request ticket number is **SR1608_04324 – WaTech – PL A9 Enterprise Security**. Based on information included in your DP and gathered during the consultation, you are seeking the creation of a new Cybersecurity Allocation and adjustments to the Enterprise Security Infrastructure Allocation to appropriately fund software, licensing, new equipment, staffing and internal agency costs. WaTech does not currently provide a service that aligns with Allocation creation or adjustments, software, licensing, the purchase of equipment, the allocation of overhead or FTEs. The Office of Cyber Security currently utilizes WaTech products and services and the additional staff being proposed will continue to use these services.

If your requirements change, please send a new request to the WaTech Service Desk at servicedesk@watech.wa.gov and include the subject line **Consultation Request for 2017-19 Biennial Budget Submittal for WaTech - PL AC Enterprise Security**.

Let me know if I can be of assistance.

Larry

Larry E. Lee
Customer Account Manager
Customer Relations Team
Washington Technology Solutions (WaTech) / Consolidated Technology Services (CTS)
360-407-8936 Office
360-480-4310 Mobile
WaTech.wa.gov

