

## 2017-19 Biennium Budget Decision Package

**Agency:** 163 - Consolidated Technology Services (WaTech)

**Decision Package Code/Title:** AE - Cybersecurity Caseload Management

**Budget Period:** 2017-19

**Budget Level:** PL – Performance Level

**Agency Recommendation Summary Text:**

Consolidated Technology Services (WaTech) requests \$1,671,000 and 4.0 FTE in the 2017-19 Biennium to address the security design review and agency assessment backlogs. The additional staff and resources will help ensure the state can provide timely assessment of agencies' security postures and accelerate the release of new, security-compliant services and applications.

**Fiscal Summary:**

<b>Operating Expenditures</b>	<b>FY 2018</b>	<b>FY 2019</b>	<b>FY 2020</b>	<b>FY 2021</b>
Fund 458-6	989,000	682,000	682,000	682,000
<b>Total Cost</b>	<b>989,000</b>	<b>682,000</b>	<b>682,000</b>	<b>682,000</b>
<b>Staffing</b>	<b>FY 2018</b>	<b>FY 2019</b>	<b>FY 2020</b>	<b>FY 2021</b>
FTEs	4.0	4.0	4.0	4.0
<b>Revenue</b>	<b>FY 2018</b>	<b>FY 2019</b>	<b>FY 2020</b>	<b>FY 2021</b>
Fund 458-6	989,000	682,000	682,000	682,000
<b>Object of Expenditure</b>	<b>FY 2018</b>	<b>FY 2019</b>	<b>FY 2020</b>	<b>FY 2021</b>
Obj. A	370,000	370,000	370,000	370,000
Obj. B	111,000	111,000	111,000	111,000
Obj. E	475,000	200,000	200,000	200,000
Obj. G	1,000	1,000	1,000	1,000
Obj. J	32,000	0	0	0

**Package Description**

The purpose of this decision package is to provide additional staffing and technical capacity to ensure Washington state government can continue to maintain the level of security and accountability its citizens and businesses expect.

In order to ensure citizen data is protected appropriately, it is imperative that online services, and the agencies that provide these services, are regularly assessed to ensure that potential vulnerabilities are identified and properly mitigated. It is also critical that data transmitted to and from the Internet is inspected, and that malicious payloads are neutralized to prevent customer client workstations and state government servers from becoming infected.

The State Office of Cyber Security (OCS) already provides effective resources that proactively identify online service and agency vulnerabilities, block malicious traffic before it reaches its destination, and expertise in security incident handling. It is imperative that these functions be able to continue to scale as an increasing number of new services are developed and the volume and sophistication of malicious threats continues to rise.

OCS provides three vital functions that support Results Washington's goal of providing efficient, effective and accountable government:

1. The Security Design Review (SDR) team is responsible for ensuring newly developed or significantly modified services and applications comply with the state's IT security standards before deployment. This critical service helps agencies make sure they get IT security "right the first time". This team conducts a detailed analysis of often very complex security architectures, and provides recommendations on how discovered vulnerabilities can be properly mitigated.
2. The Computer Emergency Readiness Team (CERT) acts in a firefighter role for the enterprise. During a cyber security incident, the team immediately mobilizes to perform incident response. The team is comprised of incident handlers, digital forensics experts and security analysts who constantly train to respond to varied cyber emergencies. When not in a firefighting role, the team performs comprehensive security assessments to assist agencies in identifying risks and making informed decisions regarding their security posture and resources.
3. To ensure malicious payloads contained in traffic between the Internet and the state network are detected and blocked, OCS uses state-of-the-art threat detection software and hardware appliances. This technology inspects traffic for code anomalies or suspected threats, and places suspicious code in a safe, offline environment where it can be executed and analyzed before reaching its destination. Code that is shown to be malicious is quarantined and erased before it can do damage to endpoint services.

Customer agencies have repeatedly expressed appreciation for the value the SDR team and CERT provide, and have come to lean on them to ensure new online services and agency IT environments are secure. They have also found that the threat detection service actually saves them time and money by eliminating the agency's need to expend IT resources on response and recovery efforts from infected devices.

The growth in the newly developed applications and the increasing need for agency assessments has created staffing capacity issues within the SDR team and the CERT. Similarly, the exponential growth of electronic traffic is close to exceeding the capabilities of the threat detection hardware and software.

The increased demand for the SDR team and the CERT has exceeded their capacity to respond in a timely and thorough manner, and created a backlog condition and delay of 2-6 months, depending on the service. Delays impact the agency's ability to meet their business needs to deliver their mission critical services in a timely manner. The backlog means that critical state agency projects are taking longer to review and analyze for IT security compliance before going live. Additionally, comprehensive IT security assessments and vulnerability remediation of individual agencies are similarly being delayed, which lowers the overall state security posture. Performing appropriate due diligence to identify and mitigate existing and newly emerging threats and vulnerabilities is still largely a staff-driven exercise, requiring numerous follow-on discussions and meetings to ensure the appropriate processes and controls are in place.

Should the capacity of the state's threat detection service be exceeded, the technology is designed to not impair business by failing open, allowing potential malicious traffic to enter the network.

**Proposed solution:**

This Decision Package will fund 4.0 FTE, and needed hardware and software licenses, in the Office of Cyber Security, at a cost of \$1,671,000 in 2017-19.

To address the security design review and agency assessment backlogs, OCS proposes that 2.0 FTE each be added to the SRD team and the CERT. This additional staff will help ensure the state can provide timely assessment of agencies' security postures and accelerate the release of new, security-compliant services and applications. Specifically, additional staff will allow multiple, concurrent, project assessment threads to be established to accelerate design reviews and agency IT security assessments.

OCS also proposes purchasing additional hardware and software licensing to extend the capacity of the threat detection platform. This will ensure consistently thorough inspection and blocking of malicious Internet code as state data traffic increases.

**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.**

The SDR team consists of three dedicated staff and one at 50 percent (or total 3.5 FTE). CERT has four full-time staff.

**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.

This proposal will expand protection of the state network through increased ability to identify, block and eliminate malicious "in-flight" code that can do harm to state and customer systems and create reputational damage to the state. It will also expand the state's existing investment in cyber defense resources and infrastructure that will protect confidential personal information and IT assets for Washington State, county and local governments.

**Performance Measure detail:**

The decision package supports the Results Washington goal #5: Efficient, Effective and Accountable Government. While the purpose of the SDR team and the CERT is to help ensure the state enterprise is accountable for the protection of electronic data and IT assets entrusted to it, the ability to improve processing time will work toward the goal of making Washington state government more effective. Threat prevention technology will 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.**

The work performed by OCS ensures the state's enterprise appropriately protects citizen data from unauthorized disclosure and protects the IT assets entrusted to it. The secure interaction of citizens

with their government is critical in delivering these vital services. However, in order to meet both the citizen's and agency's business requirements, the security assessments and reviews must be done in a timely and thorough manner. Increased staffing by 50 percent in the SDR team and CERT is expected to reduce backlog times from up to six months to less than three months without compromising the level of due diligence conducted, leading to both accountable and effective government.

**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: Impact to agencies will be positive. It will reduce the time required to review and process new IT services and conduct IT security assessments. This will help ensure that appropriate agency security controls are in place, online services are secure, and electronic protection remains sufficient to protect citizen's personally identifiable information.
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.**

This decision package will help ensure that security reviews and assessment activities conducted by OCS are delivered on a consistent, timely, and reliable basis. Agencies will be able to more accurately estimate security assessment lead time into their projects, thereby allowing them to make more realistic reliable project completion estimates. Threat detection and prevention will ensure that data maintained by the state is reliable.

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

The SDR team and CERT use specialized software whenever practicable, and these teams have made modifications to their internal and externally-facing processes with the goal of reducing time and redundancy. These efforts have had some effect, but because risk assessment and mitigation analysis requires such a high degree of human analysis, there is a limit to the degree automation and process re-design can be effective in light of increasing demand.

WaTech has conducted thorough analysis of state online traffic to determine whether certain types of online transactions could be eliminated to ensure that existing threat detection capabilities can function optimally. The result of this analysis shows that increasing levels of transactions are legitimate, and that traffic volumes will only continue to grow. In order to prevent this technology from "failing open" when traffic volume thresholds are exceeded, it is necessary to increase the capacity of the current threat detection platform.

**What are the consequences of not funding this request?**

The backlogs for comprehensive agency IT security assessment performed by the CERT and processing times for security design review of critical state IT systems will continue to impact the state's ability to deliver critical services securely and in a timely fashion, and increase the risk of exposure due to unidentified and unmitigated vulnerabilities, and will likely continue to grow.

WaTech will not be able to adequately keep pace with the expansion of IT security threats posed by adversarial parties looking to exploit vulnerabilities. Failure to do so will increase the risk of unauthorized access to critical state data assets and IT resources.

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

As mentioned previously, the SDR and CERT teams have made modifications to their internal and externally-facing processes with the goal of reducing time and redundancy. These efforts have had good effect and reduced the backlog from 3-8 months to 2-6 months. However, given the complexity of these reviews, there is a limit to what automation and process re-design can do without the need for additional staff.

**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	475,000	200,000	200,000	200,000
Staff	514,000	482,000	482,000	482,000
<b>Total Cost</b>	<b>989,000</b>	<b>682,000</b>	<b>682,000</b>	<b>682,000</b>

## 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 PL AE - Cybersecurity Caseload Management

Decision Package Cost Breakdown

Security Design Review and CERT Backlog

	# FTEs	Salary per FTE	FTE	Benefits	FY 18	FY 19	Biennial Total
				Annual Salary and Benefits			
FTEs (CERT)	2	\$ 95,000	\$ 28,500	\$ 247,000	\$ 247,000	\$ 247,000	\$ 494,000
FTEs (Design Review)	2	\$ 90,000	\$ 27,000	\$ 234,000	\$ 234,000	\$ 234,000	\$ 468,000
Travel				\$ 720	\$ 720	\$ 720	\$ 1,440
New workstations				\$ 24,000	\$ -	\$ -	\$ 24,000
CERT Workstation upgrades (2@\$2K)				\$ 4,000	\$ -	\$ -	\$ 4,000
Licenses (2 @ \$2K)				\$ 4,000	\$ -	\$ -	\$ 4,000
<b>Total</b>				<b>\$ 513,720</b>	<b>\$ 481,720</b>	<b>\$ 995,440</b>	

Threat Monitoring Capacity

	# FTEs	Salary per FTE	FTE	Benefits	FY 18	FY 19	Biennial Total
				Annual Salary and Benefits			
Appliance Purchase				\$ 475,000	\$ -	\$ -	\$ 475,000
Licensing and maintenance				\$ -	\$ 200,000	\$ 200,000	\$ 400,000
<b>Total</b>				<b>\$ 475,000</b>	<b>\$ 200,000</b>	<b>\$ 675,000</b>	
				<b>\$ 988,720</b>	<b>\$ 681,720</b>	<b>\$ 1,670,440</b>	

Expenditures	FY 2018	FY 2019	Biennium 2017-19
FTE	4.0	4.0	4.0
Object A	\$ 370,000	\$ 370,000	\$ 740,000
Object B	\$ 111,000	\$ 111,000	\$ 222,000
Object E	\$ 475,000	\$ 200,000	\$ 675,000
Object G	\$ 720	\$ 720	\$ 1,440
Object J	\$ 32,000	\$ -	\$ 32,000
<b>Total</b>	<b>\$ 988,720</b>	<b>\$ 681,720</b>	<b>\$ 1,670,440</b>

Revenue	FY 2018	FY 2019	Biennium 2017-19
Fund 458	\$ 988,720	\$ 681,720	\$ 1,670,440



## Ramos, Deborah (WaTech)

---

**From:** Lee, Larry (WaTech)  
**Sent:** Friday, August 26, 2016 5:51 PM  
**To:** Fitzgerald, Judy (WaTech); Kirk, Agnes (OCS)  
**Subject:** WaTech DP Consult for SR1608\_04257 - WaTech - PL AE Cybersecurity Caseload Management

Good afternoon Judy and Agnes,

This email is to summarize your Decision Package (DP) Consultation with WaTech. Your Service Request ticket number is **SR1608\_04257 – WaTech – PL AE Cybersecurity Caseload Management**. Based on information included in your DP and gathered during the consultation, your identified requirements include the addition of software and licensing, and new FTEs to support the package. WaTech does not currently provide a service that aligns with software, licenses and 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](mailto:servicedesk@watech.wa.gov) and include the subject line **Consultation Request for 2017-19 Biennial Budget Submittal for WaTech - PL AE Cybersecurity Caseload Management**.

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](http://WaTech.wa.gov)

