

## 2017-19 Biennium Budget Decision Package

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

**Decision Package Code/Title:** AC - Increased Cyber Defense

**Budget Period:** 2017-19

**Budget Level:** PL – Performance Level

**Agency Recommendation Summary Text:**

Consolidated Technology Services (WaTech) requests \$2,033,000 and 5.0 FTE in the 2017-19 Biennium to increase the organizational capability of the Office of Cyber Security to detect, assess, and remediate vulnerabilities across state agencies against cyber threats. This includes staff who will help agencies properly apply and configure IT security controls to withstand real-world threats, assistance for agencies to deploy effective controls that address identified vulnerabilities, and the creation of a self-service portal for agencies to more effectively monitor their own mitigation efforts and take appropriate enforcement actions.

**Fiscal Summary:**

Operating Expenditures	FY 2018	FY 2019	FY 2020	FY 2021
Fund 458-6	1,189,000	844,000	844,000	844,000
<b>Total Cost</b>	<b>1,189,000</b>	<b>844,000</b>	<b>844,000</b>	<b>844,000</b>
Staffing	FY 2018	FY 2019	FY 2020	FY 2021
FTEs	5.0	5.0	5.0	5.0
Revenue	FY 2018	FY 2019	FY 2020	FY 2021
Fund 458-6	1,189,000	844,000	844,000	844,000
Object of Expenditure	FY 2018	FY 2019	FY 2020	FY 2021
Obj. A	470,000	470,000	470,000	470,000
Obj. B	141,000	141,000	141,000	141,000
Obj. E	540,000	225,000	225,000	225,000
Obj. G	8,000	8,000	8,000	8,000
Obj. J	30,000	0	0	0

**Package Description**

The State of Washington network is under constant attack from cyber threat actors who are looking to take advantage of any single vulnerability to meet varied harmful objectives. Effective cyber defense requires that organizations continually document and adjust their security controls and processes and manage and mitigate known vulnerabilities. It is equally important that they conduct exercises against their own defenses that mimic tactics used by adversarial parties, and provide a means of threat information sharing, both inside and outside their organization.

This decision package addresses the most critical aspects of the increasingly sophisticated and persistent attack methods and tactics that put the state at risk of compromise from the hacking community, and moves Washington closer to formally adopting practices that have proven successful in the Federal government and private sector.

The cyber threat landscape continues to change and evolve as technology advances, requiring constant evaluation of defensive capabilities. While the state has effectively focused on infrastructure, the state has increasing risk in effectively protecting the data in the approximately 1300 public-facing applications as well as computer systems.

This decision package expands the state's cyber defense capabilities to allow similar focus on application and system security that we currently apply to state network and infrastructure security. The cost of not funding this extension will be to leave the state vulnerable to the fastest growing target areas for cyber-attack.

While application threat detection and assessment currently happen at a basic level, the need to identify and mitigate vulnerabilities has become even more critical. Application attacks increased 51 percent in the last year alone, the fastest growing attack vector of all incidents. Recent reports on IT security found there is a 90 percent chance of a vulnerability being exploited by an attacker if not fixed within 40 to 60 days of discovery. The reports also found that companies often leave these vulnerabilities un-mitigated for more than 120 days. This is the current situation currently at the state, and one that cannot persist without the security of state-maintained data being put at an unacceptable level of risk.

Proposed solution:

Threat actors are not going to share information about found weaknesses in our defenses with the State of Washington. Therefore it is necessary to increase organizational capability to detect, assess and remediate vulnerabilities across state agencies as well as increasing capability across the enterprise. This proposal will fund 5.0 FTE, plus hardware and software supports, in the Office of Cyber Security (OCS) at a total cost of \$2,033,000 in 2017-19.

1. It creates a cyber security "Red Team" to actively test the security of the state's networks, computer systems and online applications and services to help identify and mitigate vulnerabilities before an attack can exploit them and disrupt the delivery of government services (2.0 FTE). Any single exploit by the varied threat actors consistently probing the state network can result in significant expense and reputational harm to the state of Washington.
2. It addresses the need to provide sustainable application security patches and implementation of secure coding best practices for the approximately 1300 public-facing applications and more than 300 legacy applications that hold and/or process personally identifiable data while providing critical services to citizens and businesses.
3. Creates a real-time self-service portal for agencies to access security related information regarding an agency's security posture including vulnerability alerts, security assessment results, security design reviews and compliance data that will allow agencies to make better informed security decisions based on hard data (1.0 FTE plus development costs). It also provides the state Chief Information Officer (CIO) and Chief Information Security Officer (CISO) with an overview of the state's security posture.

4. It increases the Washington Information Sharing and Analysis Center (WA-ISAC) by 2.0 FTE. ISAC provides a vehicle for the state to collect, analyze, and disseminate actionable threat information to public organizations and with our federal partners to protect infrastructure and systems critical to the delivery of government services.

**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 Washington Information Sharing and Analysis Center (WA-ISAC) currently has only 1.0 FTE, which would be increased by an additional 2.0 FTE from this request. The remaining requests in this decision package are new capacity.

**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?**

This decision package will begin to address the state's capabilities to respond and defend against rapidly evolving cyber threats for protecting sensitive data held by state agencies and securing the delivery of online services to citizens and businesses. It will make the state safer by closing the gap between acknowledged best practices and capabilities in the private sector and the federal government, and current capabilities and practices of Washington state agencies.

Establishing the capacity to emulate hostile threat activity through the creation of the Red Team will allow the state to evaluate how well IT security controls put in place at all levels of the enterprise actually stand up to real-world hacking tactics. The ability to identify and mitigate vulnerabilities before they are actually exploited or otherwise create a significant disruption will make state data more secure. The results of Red Team testing will allow agencies to better understand how best to properly apply and configure IT security controls to withstand real-world threats.

Most importantly, however, the Red Team will also "teach us how to fish," by assisting state agencies in adopting the latest tactics in vulnerability detection, mitigation, and thinking like a modern cyber attacker.

The application patching and secure coding program will ensure that scanning, testing, remediation of found vulnerabilities and implementation of secure coding best practices are implemented for the legacy and other public-facing online applications. Mitigation assistance provided by OCS will allow agencies to rapidly deploy effective controls to address identified vulnerabilities, and help make agencies aware of existing shared IT security tools and services available.

To ensure that the benefits of the state's IT security policies and standards are realized, it is imperative that effective compliance monitoring, mitigation follow-up and enforcement take place. Better aggregation and analysis of vulnerability and compliance data through the use of a real-time portal will allow agencies to more effectively monitor mitigation efforts employed by agencies, provide the basis for appropriate enforcement actions, create comprehensive security profiles for each agency for consumption by agency heads, and provide accurate decision support for the creation of new IT security policies and services.

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.

This decision package supports the Results Washington goal of providing efficient, effective and accountable government by proactively detecting, assessing and remediating vulnerabilities across state agencies before a potential breach could impact or disrupt the delivery of state services or expose citizen data.

**Fully describe and quantify expected impacts on state residents and specific populations served.**  
The data being protected in the public-facing applications and computer systems includes personal and private information belonging to millions of Washington citizens.

**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 have expressed a desire for the OCS to provide red team testing, application secure code training, and a centralized portal to support decision making for agency security programs.
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.**

As mentioned in a previous section, agencies will benefit as a result of:

- Red Team testing that will help agencies properly apply and configure IT security controls to withstand real-world threats.
- Mitigation assistance to help agencies deploy effective controls to address identified vulnerabilities and to be aware of existing shared IT security tools and services available.
- Availability of the portal for better analysis of vulnerability and compliance data that will help agencies more effectively monitor mitigation efforts, implement appropriate enforcement actions, and provide accurate decision support for the creation of new IT security polices and services.

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

Today we are security monitors. The market warrants, and the real-life scenarios demand, that the long-term strategy be a shift to the role of security police - in other words a more active approach to handling cyber threats as is done in the private and federal sectors. As a best practice this is accomplished by centralizing all statewide security functions now handled by separate agencies. The cost of centralizing could be significant, likely \$20 million plus. Recognizing state budget realities, this is an incremental step in moving toward the long-term strategy, but at the same time improving our cyber defense capabilities.

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

The state will not be able to adequately keep pace with the increased sophistication of IT security threats posed by adversarial groups constantly attacking the state network, looking to exploit vulnerabilities and internet-facing applications. Failure to do so will increase the risk of unauthorized access to critical state data assets and IT resources and expose the state to significant financial and reputational damage.

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

There is no current capacity or funding to address this statewide risk. Absent the availability of required staff, training and tools, there are no effective means to combat the new and increasing threats the state is now encountering.

**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	325,000	175,000	175,000	175,000
Staff	864,000	669,000	669,000	669,000
<b>Total Cost</b>	<b>1,189,000</b>	<b>844,000</b>	<b>844,000</b>	<b>844,000</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:

1. Does this decision package fund the development or acquisition of a new or enhanced software or hardware system or service?  Yes  No
2. Does this decision package fund the acquisition or enhancements of any agency data centers? (See [OCIO Policy 184](#) for definition.)  Yes  No
3. 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.

Decision Package Cost Breakdown

Red Team

	# FTEs	Salary per FTE	Benefits per FTE	Annual Salary and Benefits	FY 18	FY 19	Biennial Total
FTEs	2	\$ 95,000	\$ 28,500	\$ 247,000	\$ 247,000	\$ 247,000	\$ 494,000
Travel					\$ 360	\$ 360	\$ 720
New workstations					\$ 12,000	\$ -	\$ 12,000
Tools					\$ 100,000	\$ 25,000	\$ 125,000
<b>Total</b>					<b>\$ 359,360</b>	<b>\$ 272,360</b>	<b>\$ 631,720</b>

Legacy Security Patches

	# FTEs	Salary per FTE	Benefits per FTE	Annual Salary and Benefits	FY 18	FY 19	Biennial Total
Tools					\$ 325,000	\$ 175,000	\$ 500,000
Training					\$ 25,000	\$ 25,000	\$ 50,000
<b>Total</b>					<b>\$ 350,000</b>	<b>\$ 200,000</b>	<b>\$ 550,000</b>

Security Profile Site

	# FTEs	Salary per FTE	Benefits per FTE	Annual Salary and Benefits	FY 18	FY 19	Biennial Total
FTEs	1	\$ 90,000	\$ 27,000	\$ 117,000	\$ 117,000	\$ 117,000	\$ 234,000
Travel					\$ 180	\$ 180	\$ 360
New workstations					\$ 6,000	\$ -	\$ 6,000
Development (contracted)					\$ 90,000	\$ -	\$ 90,000
<b>Total</b>					<b>\$ 213,180</b>	<b>\$ 117,180</b>	<b>\$ 330,360</b>

ISAC

	# FTEs	Salary per FTE	Benefits per FTE	Annual Salary and Benefits	FY 18	FY 19	Biennial Total
FTEs	2	\$ 95,000	\$ 28,500	\$ 247,000	\$ 247,000	\$ 247,000	\$ 494,000
Travel					\$ 7,200	\$ 7,200	\$ 14,400
New workstations					\$ 12,000	\$ -	\$ 12,000
<b>Total</b>					<b>\$ 266,200</b>	<b>\$ 254,200</b>	<b>\$ 520,400</b>
					<b>\$ 1,188,740</b>	<b>\$ 843,740</b>	<b>\$ 2,032,480</b>

Expenditures	FY 2018	FY 2019	Biennium 2017-19
FTE	5.0	5.0	5.0
Object A	\$ 470,000	\$ 470,000	\$ 940,000
Object B	\$ 141,000	\$ 141,000	\$ 282,000
Object E	\$ 540,000	\$ 225,000	\$ 765,000
Object G	\$ 7,740	\$ 7,740	\$ 15,480
Object J	\$ 30,000	\$ -	\$ 30,000
<b>Total</b>	<b>\$ 1,188,740</b>	<b>\$ 843,740</b>	<b>\$ 2,032,480</b>

Revenue	FY 2018	FY 2019	Biennium 2017-19
Fund 458	\$ 1,188,740	\$ 843,740	\$ 2,032,480



**Ramos, Deborah (WaTech)**

---

**From:** Lee, Larry (WaTech)  
**Sent:** Friday, August 26, 2016 5:55 PM  
**To:** Fitzgerald, Judy (WaTech); Kirk, Agnes (OCS)  
**Subject:** WaTech DP Consult for SR1608\_04291 - WaTech - PL AC Increased Cyber Defense

Good afternoon Judy and Agnes,

This email is to summarize your Decision Package (DP) Consultation with WaTech. Your Service Request ticket number is **SR1608\_04291 – WaTech – PL AC Increased Cyber Defense**. 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 AC Increased Cyber Defense**.

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)

