



STATE OF WASHINGTON

OFFICE OF FINANCIAL MANAGEMENT

STATE HUMAN RESOURCES DIVISION | DIRECTOR'S REVIEW PROGRAM

P.O. Box 40911 · Olympia, WA 98504-0911 · (360) 407-4101 · FAX (360) 586-4694

July 13, 2016

TO: Kristie Wilson
Acting State HR Rules and Policy Manager

FROM: Kris Brophy
Director's Review Specialist

SUBJECT: Curtis McDaniel v. Washington State Patrol (WSP)
Allocation Review Request ALLO-16-015

Director's Determination

This position review was based on the work performed for the six-month period prior to July 14, 2015, the date WSP Human Resources (WSP HR) received Mr. McDaniel's request for a position review. As the Director's Review Specialist, I carefully considered all of the documentation in the file, the exhibits and the verbal comments provided by both parties. Based on my review and analysis of Mr. McDaniel's assigned duties and responsibilities, I conclude his position is properly allocated to the Information Technology Specialist 4 (ITS 4) classification.

Background

On July 14, 2015, WSP HR received Mr. McDaniel's Position Review Request (PRR), asking that his position be reallocated to the Information Technology Specialist 5 (ITS 5) class. (Exhibit B-5)

On February 24, 2016, WSP HR notified Mr. McDaniel that his position was properly allocated to the ITS 4 class. (Exhibit B-1)

On March 9, 2016, OFM – State HR received Mr. McDaniel's request for a Director's review of WSP's allocation determination. (Exhibit A-1)

On July 7, 2016, I conducted a Director's review telephone conference. Present for the conference were Curtis McDaniel; Patrick Neville, Staff Representative, WPEA; Mike Geiger, Engineering Section Manager, WSP; Stu Lundmark, ITS 6 Network Security Manager, WSP, Captain Travis Matheson, WSP; Dr. Ben Lastimado, HR Operations Manager, WSP; Debb Tindall, HR Program Manager, WSP; Melissa Rasmussen, HR Consultant, WSP; and Melodie Wulfekuhle, HR Consultant, WSP.

Rationale for Director's Determination

The purpose of a position review is to determine which classification best describes the overall duties and responsibilities of a position. A position review is neither a measurement of the volume of work performed, nor an evaluation of the expertise with which that work is performed. A position review is a comparison of the duties and responsibilities of a particular position to the available classification specifications. This review results in a determination of the class that best describes the overall duties and responsibilities of the position. *Liddle-Stamper v. Washington State University*, PAB Case No. 3722-A2 (1994).

Organizational Structure

Mr. McDaniel serves as the Network Security Administrator for Network Security Group located within the Electronic Services Division (ESD) of WSP. His position reports to Stu Lundmark, Network Security Manager, who in turn reports to Mike Geiger, Engineering Section Manager.

Position Purpose

In the Position Review Request (PRR) submitted for reallocation, Mr. McDaniel states in the Position Purpose section that (Exhibit B-5):

My position serves as the administrator for the WSP Agency Intrusion Prevention System, WebSense Web Security Gateway, Adaptive Security Appliances located throughout the state, Remote Access Virtual Private Network and Cisco Identity Services Engine. It is responsible for network trouble shooting, hardware and software installation, and training staff. My position determines when software upgrades are necessary, makes recommendations for hardware replacement and makes purchasing recommendations.

Duties and Responsibilities

Mr. McDaniel describes his duties in the PRR as follows:

25% Duty:

Cisco Access Control Server (ACS) and Cisco Identity Services Engine (ISE)

Tasks:

Supports, maintains and enhances existing, high risk and impact, mission critical WSP data and network resources are available with proper authentication and authorization of WSP users and computers. Cisco ACS controls WSP Network Staff access to all WSP network equipment; Cisco ISE controls WSP Staff and Business Partners access to WSP Network resources from Remote Access, VPN and Wireless.

Identify and independently resolve operational problems for mission critical resources that rely upon correct user and computer authentication and authorization rules.

Modify Access-Lists to allow network communication between authorized users and WSP network resources or external resources while denying access to resources not authorized for.

Add or modify current Authentication and Authorization rules in Cisco ISE for all VPN's, new Wireless system, Cisco phones etc. All devices in the WSP network require some form of endpoint profile in the ISE.

It is expected that Cisco ISE will be the Authentication and Authorization System providing access to WSP for all future expansion/technologies including Bring-Your-Own-Device (BYOD).

Analyze and recommend new capabilities/technologies that may be applied to the WSP. Provide documented testing along with cost estimates of new products that will replace or upgrade existing hardware and software solutions.

25% **Duty:**

Cisco ASA and PIX Firewall

Tasks:

Monitor logs for excessive/suspicious denied activity within the WSP network and to or from the WSP network and external sources.

Modify Access-Lists to allow network communication between authorized users and WSP network resources or external resources while denying access to resources not authorized for.

Review new application information to determine if new rules are needed.

Identify and independently resolve operational problems and/or very complex problems such as multiple product problems or conflicts caused by new hardware, software or configurations modified on networks not under WSP control.

Review published updates and schedule updates if required.

25% **Duty:**

Cisco Virtual Private Network (VPN).

Tasks:

Supports, maintains and enhances existing, high risk and impact, mission critical WSP data and network resources are available through the Cisco VPN.

Identify and independently resolve operational problems for the mission critical VPN network that provides support for WSP, DOT, DOL, DOC, OIC and other Federal and State Agencies that access WSP resources through our VPN.

Analyze and recommend new capabilities/technologies that may be applied to the WSP. Provide documented testing along with cost estimates of new products that will replace or upgrade existing hardware and software VPN solutions.

20% **Duty:**

WebSense Web Security Gateway

Tasks:

Monitoring Internet access to/from Security Risk Category sites.

Adding/removing/modifying Delegated Administrators for WebSense. There are currently 41 Administrators in 31 Admin Groups.

Implement the technical policies for the WSP Internet usage by customizing categories and business-related websites for WSP access and modifying user policies to permit/deny access to specific Internet sites/categories in WebSense. Currently over 2200 users and more than 200 servers accessing the billion sites on the World Wide Web.

Review current Security Alert Bulletins to determine if WSP users are attempting to go to compromised sites.

Review published updates to determine if WSP requires the update. If required then schedule the update with all departments needed to accomplish the update.

5% **Duty:**

Cisco Intrusion Prevention System (IPS)

Tasks:

Monitor logs for excessive/suspicious denied activity within the WSP network and to or from the WSP network and external sources.

Modify IPS Signatures to prevent false positive triggers from blocking normal traffic. Allow normal communication between authorized users and WSP network resources or external resources while denying access to resources that have triggered a signature that could cause a network denial of service or download Trojans or other malware from an infected site.

Review new application information to determine if the existing configuration will permit or block normal application behavior.

Identify and independently resolve operational problems and/or very complex problems such as multiple product problems or conflicts caused by new hardware, software or configurations modified on networks not under WSP control.

Review published updates and schedule updates if required.

Supervisor's Comments

Mr. Lundmark completed the Supervisor Portion of the PRR. (Exhibit B-6)

Mr. Lundmark indicates that Mr. McDaniel's description of his assigned duties and responsibilities in the Work Activities section of the PRR is not fully accurate and complete.

He states:

Curt troubleshoots and resolves NOC, WSP ACCESS, WSP AFIS, server/application access and general network problems at a high level.

All these problems may be under the umbrella of the duties he listed. I am listing it separate here. This also would include his "lead" expertise for NOC and for assisting the ITD Help Desk.

Curt responds to complex, network issues forwarded by NOC, ITD Help Desk, ITD Server Support and ITD Application and other ESD staff in general.

The ITD Server and ITD Application support is generally a very integrated network-server-app system that is experiencing a problem, possibly network security related.

WSP ACCESS and WSP AFIS problem solving is always related to outside entities having trouble connecting to WSP. I estimate this to be about 20% of his time.

Mr. Lundmark indicates that Mr. McDaniel's position does not have designated lead or supervisory responsibility over other ITS staff. He also provides the following comments regarding the scope of Mr. McDaniel's decision making authority:

Under CISCO ISE and Authentication area:

Agency IT approved architecture has determined the guidelines. How it gets configured internally and implemented to meet those requirements is Curt's decision.

Under Web Security Gateway area:

There are multiple policy areas within the Web Security Gateway. Risk Management Division dictates the policy pertaining to allowable and forbidden web site content, and Curt enforces that policy.

Mr. Lundmark provides the following examples of decisions Mr. McDaniel is authorized to make without his prior review:

Security threat responses that are based on individual workstations, servers or websites.

This would be analyzing the situation, extent of problem, interacting with the affected users and ITD, and then taking appropriate action. There is no WSP manual, or script to follow in the initial stages of an initial IT security breach or event other than determine what it is, extent, affected systems and users. The initial response is based on experience, general WSP operational knowledge and WSP system knowledge. Curt has to make quick decisions. The IT Threat landscape is constantly changing. Web Security Gateway security policy changes invoked by vendor may be overridden by Curt if he determines the vendor action was in error, or did not warrant a WSP action.

Mr. Lundmark also stated that security threats that are large, or global or where the threat response could have an impact on all WSP would require his prior approval.

Summary of Mr. McDaniel's Perspective

The argument presented by Mr. McDaniel is summarized as follows:

- He is the expert individual that other IT professionals within the WSP consult with for issues or planning out enterprise or organization-wide technology improvements.
- He serves as the system administrator for five WSP mission-critical systems. These are agency-wide systems which reach the requirements of the ITS 5 class.
- He is involved with the following equipment within the WSP Network Group Electronic Services Division: Routers, Switches, Firewalls, Virtual Private Network hardware, Intrusion Prevention Sensors, Cisco Access Control and Cisco Identity Services Engine (ISE) and the WebSense Internet Web Security Gateway.
- The ESD Network Security Group is currently understaffed and he is performing those functions as well as having responsibility for serving as the Lead for assigned ITS-3 and ITS-4 personnel.
- There are other positions within the agency performing similar work that are allocated to the ITS 5 class.
- In total, his duties and responsibilities are best described by the ITS 5 class.

In *Byrnes v. Dept's of Personnel and Corrections*, PRB No. R-ALLO-06-005 (2006), the Board held that "[w]hile a comparison of one position to another similar position may be useful in gaining a better understanding of the duties performed by and the level of responsibility assigned to an incumbent, allocation of a position must be based on the overall duties and responsibilities assigned to an individual position compared to the existing classifications. The allocation or misallocation of a similar position is not a determining factor in the appropriate allocation of a position." Citing to *Flahaut v. Dept's of Personnel and Labor and Industries*, PAB No. ALLO 96-0009 (1996).

Summary of WSP's Perspective

The argument presented by WSP is summarized as follows:

- The network security systems that he monitors are mission-critical systems because they impact the network security of the Agency. However, his position fits within a work group consisting of ITS positions with varying degrees of responsibility.
- Mr. McDaniel's supervisor, Stu Lundmark, has been assigned the responsibility of serving as the IT Network Security Manager, while Mr. McDaniel serves as a senior level position.
- As the senior network analyst, it is clear that Mr. McDaniel has tremendous responsibility and an important role in supporting and maintaining critical systems that keep WSP operations running smoothly. However, the level of responsibility assigned to Mr. McDaniel's position fits the senior specialist level.
- In total, his duties and responsibilities are best described by the ITS 4 class.

Comparison of Duties to Class Specifications

When comparing the assignment of work and level of responsibility to the available class specifications, the class series concept (if one exists) followed by definition and distinguishing characteristics are primary considerations. While examples of typical work identified in a class specification do not form the basis for an allocation, they lend support to the work envisioned within a classification.

Comparison of Duties to Information Technology Specialist series

The Class Series Concept for this series states:

Positions in this category perform professional information technology systems and/or applications support for client applications, databases, computer hardware and software products, network infrastructure equipment, or telecommunications software or hardware.

This category broadly describes positions in one or more information technology disciplines such as: Application Development And Maintenance, Application Testing, Capacity Planning, Business Analysis and/or Process Re-Engineering, Data Base Design And Maintenance, Data Communications, Disaster Recovery/Data Security, Distributed Systems/LAN/WAN/PC, Hardware Management And Support, Network Operations, Production Control, Quality Assurance, IT Project Management, Systems Software, Web Development, or Voice Communications.

Positions which perform information technology-related work to accomplish tasks but are non-technical in nature would not be included in this occupational category.

Mr. McDaniel's position performs professional Information Technology network security support. His position serves as the administrator for the WSP Agency Intrusion Prevention System, WebSense Web Security Gateway, Adaptive Security Appliances located throughout the state, Remote Access Virtual Private Network and Cisco Identity Services Engine. Mr. McDaniel's position should be allocated to a class within the Information Technology Specialist series.

Comparison of Duties to Information Technology Specialist 5 (ITS 5)

The Definition for this class states:

This is the supervisory or expert level. Provides expert consultation and specialized analysis, design, development, acquisition, installation, maintenance, programming, testing, quality assurance, troubleshooting, and/or problem resolution tasks for major organization-wide, high risk/high impact, or mission-critical applications computing and/or telecommunication systems, projects, databases or database management systems; support products, or operational problems.

Performs highly-complex tasks such as conducting capacity planning to determine organization-wide needs and make recommendations; designing complex agency- or institution-wide enterprise systems crossing multiple networks, platforms or telecommunication environments;

overseeing the daily operations of large-scale or enterprise systems; identifying and resolving operational problems for major high risk systems with centralized, organization-wide functions; testing multi-dimensional applications, providing quality assurance; developing standards or enhancing existing, high risk and impact, mission critical applications; integrating business solutions, or writing feasibility studies and decision packages for high visibility/impact initiatives.

Provides leadership and expert consultation for large-scale projects or enterprise systems that often integrate new technology and/or carry out organization-wide information technology functions, or impact other institutions or agencies. Provides project management leadership, technical expertise and demonstrates knowledge of project management practices, principles, and skills.

May supervise information technology specialists or function as a recognized expert who is sought out by others in resolving or assessing controversial or precedent-setting issues.

There are no Distinguishing Characteristics for this class.

The State HR, *Glossary of Classification Terms* defines "Expert" as follows:

Expert - Within the context of the class series, has the highest level of responsibility and extensive knowledge based on research and experience in a specific area. Resolves the most complex, critical or precedent-setting issues that arise. Positions act as a resource and provide guidance on specialized technical issues. Although an employee may be considered by their peers as an expert or "go-to" person at any level, for purposes of allocation, the term is typically applied to an employee in a higher class level who has gained expertise through progression in the series.

While a portion of Mr. McDaniel's work involves performing some duties which reach aspects of work performed by this class, in total, the majority of his work does not reach the ITS 5 level of responsibility.

Highly-complex Tasks

Incumbents in this class spend a majority of their time performing highly-complex tasks requiring highly-specialized technical knowledge and understanding of complex computing environment(s) and their client's needs. Incumbents perform such tasks as designing enterprise-level or other large-scale systems which extend beyond an assigned area of responsibility as noted at the ITS 4 level.

At this level incumbents have discretion and are delegated authority in their role as an expert-level specialist to resolve the most complex operational problems for major high-risk systems that often have centralized or organization-wide functions; have delegated authority to make decisions affecting project or operational outcomes which often go beyond divisional lines. Performance at this level is evaluated in terms of adherence to program goals, budgetary limitations, compliance with laws and regulations and general organizational policy.

Mr. McDaniel identifies and independently resolves operational problems for mission critical network security applications that rely upon correct user and computer authentication and authorization rules. During the review telephone conference Mr. Geiger acknowledged that Mr. McDaniel supports mission-critical network security application systems for the agency. This portion of his work reaches certain aspects of resolving complex operational problems for mission critical systems. However, the overall scope and level of his responsibility more accurately aligns with performing senior-level ITS 4 work which involves, "identifying and resolving multiple-server problems, transmission problems and working with vendors to solve complex problems that can only be resolved at the vendor level".

Mr. McDaniel's position does not have primary or lead responsibility for designing enterprise-level systems crossing divisional lines with multiple networks, platforms, or telecommunication environments. This level of work is performed by higher level IT staff. For example, Mr. Lundmark states in his comments that with respect to the CISCO ISE and Authentication area, agency-approved IT systems architecture is already in place and Mr. McDaniel follows established guidelines to independently determine how to configure and implement changes to meet changing requirements.

Further, Mr. McDaniel is not responsible for conducting capacity planning to determine organization-wide needs nor does he have primary responsibility for developing project plans and directing large-scale projects for the WSP ESD Network Security Group systems. During the review conference Mr. Lundmark stated that he is responsible for performing this function as the IT Security Manager for the ESD Network Security Group.

Project Leadership and Expert Consultation.

Incumbents at the ITS 5 level also provide leadership and expert-level consultation for large-scale projects or enterprise systems that often integrate new technology and/or carry out organization-wide information technology functions, or impact other agencies. Incumbents exercise broad discretion and authority in their role as expert-level specialists and are generally delegated decision-making authority across divisional lines. Mr. McDaniel's position partially reaches this overall level of responsibility.

For example, the security applications Mr. McDaniel supports provides network security for the agency. Mr. McDaniel's position requires extensive knowledge in order to analyze and resolve complex network security operational issues, which includes analyzing impacts to other systems. He also analyzes and recommends new capabilities/technologies that may be applied to the WSP. He provides cost estimates of new products that will replace or upgrade existing software solutions.

However, Mr. McDaniel's decision making authority is limited to resolving operational problems. He is also included in discussions with management about network security enhancements, but does not have authority to make decisions at that level. This responsibility rests with his supervisor and higher level management staff within ESD.

From the information and exhibits presented, Mr. McDaniel's responsibilities are more tactically focused, primarily focusing on administering the ESD's network security operations. Mr. McDaniel's position, provides senior-level systems operation and network administrator support. Overall, the scope of his work does not reach the ITS 5 level of responsibility for providing project leadership and expert-level consultation and guidance for large-scale projects or enterprise systems that often integrate new technology and/or carry out organization-wide information technology functions, or impact other institutions or agencies.

In total, Mr. McDaniel's position does not have the scope of responsibility for performing ITS 5 level work. This is supported in Pogue and Goshorn v. Labor and Industries, PRB Case Nos. R-Allo-07-017 & R-Allo-07-018 (2008) which state in relevant part:

... Appellants do not perform highly-complex tasks with the breadth of impact envisioned by the ITS5 classification. While Appellants' work impacts all employers and recipients of certain benefits, their work does not impact L&I on an organization-wide level. For example, Appellants do not conduct capacity planning to determine organization-wide needs; design complex agency-wide enterprise systems crossing multiple networks, platforms or telecommunication environments; or identify and resolve operational problems for major high risk systems with centralized, organization-wide functions. While Appellants provide leadership and expert consultation in their assigned areas, they do not perform these functions for large-scale projects or enterprise systems involving organization-wide information technology functions. Duties performed at an organization-wide level would potentially impact all business areas within an agency. Appellant's work impacts Claims Administration; their work does not impact all of L&I's business areas.

Therefore, Mr. McDaniel's position does not encompass the full scope and level of responsibility required by this class. For these reasons, his position should not be allocated to the ITS 5 class.

Comparison of Duties to Information Technology Specialist 4 (ITS 4)

The Definition for this class states:

Performs analysis, system design, acquisition, installation, maintenance, programming, project management, quality assurance, troubleshooting, problem resolution, and/or consulting tasks for complex computing system, application, data access/retrieval, multi-functional databases or database management systems, telecommunication, project or operational problems.

As a senior-level specialist in an assigned area of responsibility and/or as a team or project leader, applies advanced technical knowledge and considerable discretion to evaluate and resolve complex tasks such as planning and directing large-scale projects; conducting capacity planning; designing multiple-server systems; directing or facilitating the installation of complex systems, hardware, software, application interfaces, or applications; developing and implementing quality assurance testing and performance monitoring; planning, administering, and coordinating organization-wide information technology training; acting as a liaison on the development of applications; representing institution-wide computing and/or telecommunication standards and philosophy at meetings; or developing security policies and standards.

Incumbents understand the customer's business from the perspective of a senior business person and are conversant in the customer's business language. Projects assigned to this level impact geographical groupings of offices/facilities, and/or regional, divisional, or multiple business units with multiple functions. The majority of tasks performed have wide-area impact, integrate new technology, and/or affect how the mission is accomplished.

There are no Distinguishing Characteristics for this class.

The primary thrust of Mr. McDaniel's position, and the majority of his duties as a whole, more accurately align with the scope and level of responsibility stated in the Definition of this class.

For example, Mr. McDaniel serves as the system administrator for five ESD network security systems. He performs senior-level level IT systems administration work supporting the ESD's Virtual Private Network hardware, Intrusion Prevention Sensors, Cisco Access Control and Cisco Identity Services Engine (ISE) and the WebSense Internet Web Security Gateway.

Mr. McDaniel's position provides technical consultation and support to network security applications that are primarily implemented across multiple business units and client agencies, which is consistent with the Definition of this class for independently resolving complex computing needs within an assigned area of responsibility. Mr. McDaniel's position encompasses an area of responsibility which impacts, "...divisional, or multiple business units with multiple functions."

Mr. McDaniel performs senior-level information technology network security systems administration. Mr. McDaniel spends the majority of his time performing senior level systems administration work. This includes providing technical assistance, training and resolving complex problems and performing other related tasks at a level consistent with the Definition of this class.

Although the Typical Work examples do not form the basis for an allocation, they lend support to the work envisioned within a classification. The following are examples of work assigned to the ITS 4 class, as stated on the class specification:

Conducts capacity planning to determine the needs of an assigned area. Analyzes new capabilities that may be applied. Tests and evaluates new software and/or hardware products, document characteristics, and make recommendations;

Identifies and resolves multiple-server problems, transmission problems, etc. Works with vendors to solve complex problems. Uses advanced diagnostic tools to analyze work of others and personally resolve complex problems. Leads problem solving teams;

Acts as a liaison on the development of applications and modifications to existing applications. Represents organization-wide computing standards and philosophy at meetings, and reports information back to unit administrators;

Develops and implements quality assurance testing and performance monitoring, utilizing quality assurance techniques and practices;

Conducts traffic studies, analyzes information and trends, makes recommendations and takes action to improve system performance and efficiency;

Assesses and develops training materials and conducts advanced instruction on the use of information technologies.

Develops security policies and standards. Tests and installs security systems. Analyzes and designs security access. Establishes and implements security environments and risk-based access profiles such as firewalls. Analyzes security reports, billings, etc. to detect violations or intrusions. Provides required security access. Conducts security awareness training;

...

Mr. McDaniel's duties are fully consistent with these statements. His duties include planning with agency management staff and assisting in implementing changes in the network security function. Mr. McDaniel works with established vendors to respond to problems related to hardware/software. He tests, installs and monitors security systems. He analyzes and designs security access. He assists in establishing and implementing security environments and risk-based access profiles such as firewalls. His duties include analyzing security reports to detect violations or intrusions.

For example, Mr. McDaniel performs the following tasks as stated in the PRR:

- He modifies Access-Lists to allow network communication between authorized users and WSP network resources or external resources and denies access to unauthorized resources.
- He monitors logs for excessive or suspicious denied activity within the WSP network and to or from the WSP network and external sources.
- He identifies and independently resolves operational and other complex problems such as multiple product problems or conflicts caused by new hardware, software or configurations modified on networks not under WSP control.
- He implements technical policies for the WSP Internet usage by customizing categories and business-related websites for WSP access and modifies user policies to permit or deny access to specific Internet sites/categories in WebSense.
- He reviews current Security Alert Bulletins to determine if WSP users are attempting to go to compromised sites.
- He modifies IPS Signatures to prevent false positive triggers from blocking normal traffic. He allows normal communication between authorized users and WSP network resources or external resources while denying access to resources that have triggered a signature that could cause a network denial of service or download Trojans or other malware from an infected site.
- He reviews new application information to determine if the existing configuration will permit or block normal application behavior.
- He reviews and schedules published updates and schedules with departments if required.

When determining the appropriate classification for a specific position, the duties and responsibilities of that position must be considered in their entirety and the position must be allocated to the classification that provides the best fit overall for the majority of the position's duties and responsibilities. *Dudley v. Dept. of Labor and Industries*, PRB Case No. R-ALLO-07-007 (2007).

In this case, the majority and focus of his work and level of responsibility more fully align with the work described by the Information Technology Specialist 4 classification. Mr. McDaniel's position should remain allocated to that class.

Appeal Rights

RCW 41.06.170 governs the right to appeal. RCW 41.06.170(4) provides, in relevant part, the following:

An employee incumbent in a position at the time of its allocation or reallocation, or the agency utilizing the position, may appeal the allocation or reallocation to the Washington personnel resources board. Notice of such appeal must be filed in writing within thirty days of the action from which appeal is taken.

The mailing address for the Personnel Resources Board (PRB) is PO Box 40911, Olympia, Washington, 98504-0911. The PRB Office is located on the 3rd floor of the Raad Building, 128 10th Avenue SW, Olympia, Washington. The main telephone number is (360) 407-4101 and the fax number is (360) 586-4694.

If no further action is taken, the Director's determination becomes final.

c: Curtis McDaniel
Patrick Neville, WPEA
Dr. Ben Lastimado, WSP

Enclosure: List of Exhibits

CURTIS McDANIEL v WSP

ALLO-16-015

LIST OF EXHIBITS

A. Curtis McDaniel Exhibits

1. Director's Review Form received March 9, 2016
2. Cover Page with additional information sent with Director Review request
3. Supplemental Information for Review sent April 28, 2016

B. WSP Exhibits

1. Allocation Determination Letter sent to Mr. Curtis W. McDaniel dated 2/24/16
2. Allocation Determination Letter sent to Mr. Stuart Lundmark (direct Supervisor) dated 2/24/16
3. Allocation Analysis with signatures from HR Allocation Team dated 2/23/16
4. Email from Section Manager with agreement to the Assessment dated 2/19/16
5. Position Review Request – Employee Portion date stamped into HR 7/14/15
6. Position Review Request – Supervisor Portion date stamped into HR 8/14/15 (accompanied by copy of Employee Portion)
7. Desk Audit Questionnaire – Employee Portion by Melissa Rasmussen dated 11/5/15
8. Desk Audit Questionnaire – Employee Portion by Melodie Wulfekuhle dated 11/5/15
9. Web Design diagram – provided as work sample by Mr. McDaniel during desk audit
10. Desk Audit Questionnaire – Supervisor Portion
11. Desk Audit Questionnaire for Supervisor – notes by Melissa Rasmussen dated 11/5/15
12. Desk Audit Questionnaire for Supervisor – notes by Melodie Wulfekuhle dated 11/5/15
13. Current Position Description Form – Position #1289 signed 12/31/13
14. IT Class Restructure Proposed Position Description Form with Org Chart – Position 1289 signed 8/14/15
15. Org Chart dated July 2015 – position highlighted in yellow
16. State of Washington Class Specification – Information Technology Specialist 4
17. State of Washington Class Specification – Information Technology Specialist 5

C. State HR Class Specifications

1. Information Technology Specialist 1
2. Information Technology Specialist 4
3. Information Technology Specialist 5