REPORT DOCUMENTATION PAGE

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
31-03-2017	Technical, Final	5/12/2015 - 12/31/2016

4. TITLE AND SUBTITLE
Cybersecurity Workforce Development and the Protection of Critical Infrastructure

5a. CONTRACT NUMBER
N00014-15-1-2407

5b. GRANT NUMBER
GRANT11858219

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Matthew A. Chapman

5d. PROJECT NUMBER
1000000826

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
University of Hawaii - System
University of Hawaii - West Oahu
96-129 Ala Ike
Pearl City, Hawaii 96782-3626

8. PERFORMING ORGANIZATION REPORT NUMBER
Cyber-ONR-2015-1

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Richard Carlin, 33
Office of Naval Research
875 N. Randolf Street, Suite 1425
Arlington, VA 22203-1995

10. SPONSOR/MONITOR'S ACRONYM(S)
ONR N63374

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Unlimited Distribution

13. SUPPLEMENTARY NOTES

14. ABSTRACT
This Cyber Security Workforce Development Project directly supports workforce development needs for the U.S. Navy; promotes local, regional, and global needs to develop subject matter experts in information security and assurance; and supports the transition of veterans into engineering related career fields. Funding to support the three lines of effort described here, expansion of the UHWO Cyber Security Coordination Center (UHWO CSCC), establishment of the UHWO CSCC Network Vulnerability Assessment Lab, and the Expansion of the Troops to Engineers Program was instrumental to the success of this project and the further development of the cybersecurity workforce.

15. SUBJECT TERMS
Cybersecurity
Workforce Development
Information Security

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Matthew A. Chapman
U	U	U	UU		19b. TELEPHONE NUMBER (Include area code) 808-689-2333

UNIVERSITY of HAWAI'I°
WEST O'AHU

Final Project Technical Report:

Cyber Security Workforce Development and the Protection of Critical Infrastructure

Principal Manager / Primary Investigator:

Matthew A. Chapman, Ph.D.,
Associate Professor of Information Technology & Cybersecurity
University of Hawai'i West O'ahu
Phone: 808-689-2333
Email: mchapman@hawaii.edu

Technical contact:
Melody Bentz
Contracts & Grants Specialist
University of Hawaii West Oahu
91-1001 Farrington Hwy
Kapolei, HI 96707
Phone: 808-689-2324
Fax: 808-956-9081
Email: mbentz@hawaii.edu

Business Contact:
Sharon Mitani
Fiscal Administrator for Grants
University of Hawaii West Oahu
91-1001 Farrington Hwy
Kapolei, HI 96707
Phone: 808-689-2505
Fax: 808-689-2501
Email: mitani@hawaii.edu

Proposed Period of Performance: May 15th, 2015 – December 31st, 2016

Executive Summary

Based on the rapid expansion of cyberspace operations and the importance of cyber security to both the Department of Defense (DoD) and industry, the University of Hawai'i - West O'ahu (UHWO) developed the Bachelor of Applied Science degree with a concentration in Information Security and Assurance (BAS-ISA). The mission of the program is to:

> *"Prepare all students, including Native Hawaiian, local, and regional students for employment in the information technology and information security career fields upon graduation."*

This Cyber Security Workforce Development and the Protection of Critical Infrastructure Project directly supports workforce development needs for the U.S. Navy; promotes local, regional, and global needs to develop subject matter experts in information security and assurance; and supports the transition of veterans into engineering related career fields. The project was completed along three lines of effort: expansion of the UHWO Cyber Security Coordination Center (UHWO CSCC), establishment of the UHWO CSCC Network Vulnerability Assessment Lab, and the Expansion of the Troops to Engineers Program. The estimated and final cost for the program was $360,275.

UNIVERSITY of HAWAI'I WEST O'AHU — **UH West O'ahu** — UNIVERSITY of HAWAI'I WEST O'AHU

EXPENDITURES

ONR Cyber Center Associated Grants Since 2013

Cyber	$-	$-	$360,275	$159,625	$141,383	$143,100
Year	2013	2014	2015	2016	2017	2018

CYBERSECURITY ACCOMPLISHMENTS

Grant Award (05/15/15 – 12/14/16)
- Expansion of the UHWO Cyber Security Coordination Center (UHWO CSCC)
- Establishment of the UHWO CSCC Network Vulnerability Assessment Lab

Grant Award (08/15/16 – 08/14/19)
- Sustainment of the UHWO Cyber Security Coordination Center
- Sustainment of the UHWO CSCC Network Vulnerability Assessment Lab

NSA/DHS Certified National Center of Academic Excellence in Cyber Defense Education through Academic Year 2021

National Cyber League Champions - 2016

PROGRAM DESCRIPTION

Organization: UH West O'ahu

Primary Investigator: Dr. Matthew Chapman

Summary:
- Cyber Security Workforce Development and the Protection of Critical Infrastructure
- Expanded physical Cyber Security Coordination Center (CSCC) with public accessible web-portal
- Partnership with SPAWAR Systems Center Pacific

Table of Contents

Introduction

Since 1976, the University of Hawai'i - West O'ahu (UHWO) has served the people of Hawai'i and remains a dynamic and diverse place of learning and cultural enrichment. UHWO is located in the city of Kapolei on the island of O'ahu, and is a four-year, comprehensive university with an emphasis on career-related baccalaureate education based on state, regional, and global needs. The university is located closely to key defense and military facilities to include: Joint Base Pearl Harbor-Hickam, Headquarters United States Pacific, Command, Schofield Barracks, Kaneohe Marine Corps Base, and numerous critical Department of Defense (DoD) facilities.

Due to the rapid expansion of cyberspace operations and the importance of cyber security for both the DoD and industry, UHWO developed the Bachelor of Applied Science degree with a concentration in Information Security and Assurance (BAS-ISA). This degree program is the first of its kind at a public institution in Hawai'i and the Pacific to be developed in response to both national and state needs for graduates with education in information security. The concentration was developed in cooperation with University of Hawaii Community Colleges, state and federal law enforcement agencies, state security officials, and local businesses to cover a wide variety of technical and managerial aspects within the field.

The National Security Agency (NSA) and the Department of Homeland Defense (DHS) have certified the University of Hawai'i - West O'ahu as a National Center of Academic Excellence in cyber defense education through academic year 2021. This is in keeping with the mission and vision of the information technology and security concentrations at UHWO.

> *"Prepare all students, including Native Hawaiian, local, and regional students for employment in the information technology and information security career fields upon graduation (Mission)."*

> *"Establish and expand the UHWO Cyber Security Coordination Center as a Center of Academic Excellence in Information Security and Cyber Defense, educating students to be engaged global citizens and leaders in our society (Vision)."*

Additionally, the Chief of Naval Operations (CNO) Position Report for 2014 highlighted the U.S. Navy's plan to develop a cadre of about 1,000 cyberspace operators by 2016 to man cyber mission teams and identifies other personnel shortfalls that may directly impact readiness.

Project Objective

This Cyber Security Workforce Development and the Protection of Critical Infrastructure Project directly supports workforce development needs for the U.S. Navy; promotes local, regional, and global needs to develop subject matter experts in information security and assurance; and supports the transition of veterans into engineering related career fields. Funding to support the three lines of effort described here, expansion of the UHWO Cyber Security

Coordination Center (UHWO CSCC), establishment of the UHWO CSCC Network Vulnerability Assessment Lab, and the Expansion of the Troops to Engineers Program was instrumental to the success of this project and for progressing towards the stated mission and vision for the BAS-ISA program. The estimated and actual cost of this complete project was $360,275, which includes the three lines of effort and project management requirements.

Technical Findings

Expansion of the UHWO Cyber Security Coordination Center (UHWO CSCC)

The purpose of the UHWO CSCC is to provide BAS-ISA students with an opportunity to work in a cyber-operations center and coordinate cyber defense information with local and regional partners. This center provides students with experience and education as network defense subject matter experts to prepare them for future employment in industry or the DoD. This center also supports information security needs in the community and region by acting as a resource to learn about modern cyber conflicts emerging threats. Curriculum courses that support this center include Proactive System Security, Digital Forensics, Management of Information Security, Modern Cyber Conflicts, and Senior Practicum. The expansion of the center supports the NSA/DHS National Centers of Academic Excellence focus areas of Cyber Investigations and Security Incident Analysis and Response.

This program has been expanded and now includes a further developed web-based coordination site, associated hardware, and software for the on-campus UHWO CSCC, administrative stipends for practicum and research students, faculty summer salary, communications products, and limited travel for site visits and conferencing.

The CSCC contains a developed web-based coordination site, computer workstations, and industry standard software for interns to conduct their research. Currently, the CSCC is located on the UHWO campus in Building E, and is staffed with five student research interns performing the following roles: Global Cyber Environment Analyst, Vulnerability Researcher, Best Practices Analyst, Forensics Analyst, and Industrial Control Systems Cybersecurity Analyst.

The *Global Cyber Analyst* position researches and conduct analysis on current national and international developments related to cybersecurity. This involves gathering information on activities such as data breaches, cyber-related legislative activities, and international and domestic events. The duty requirements for this position include:

- Production of weekly executive summaries.
- Maintenance of designated web space with current analysis.
- Maintenance of information security resources for the CSCC.

The *Best Practices Analyst* position maintains a list of best practices, computer related patches, and standard operating procedures (SOP) for various Operating Systems (OS), software and hardware. The duty requirements for this position include:

- Keep up to date with latest patches and security updates for Linux Windows, and Mac OSs.
- Maintain a list of SOPs for hardening Linux Windows, and Mac OS.
- Provide weekly executive summaries of software updates and patches for the CSCC.
- Maintain a list of updates and patch resources for the CSCC.

The *Vulnerability Researcher* position investigates the latest security vulnerabilities and published exploits. The Vulnerability Researcher analyzes the vulnerabilities and exploits to provide information on how they work, the likelihood of it turning into an attack, and how to best mitigate the issue. The duty requirements for this position include:

- Research the latest vulnerabilities and exploits.
- Test and document vulnerabilities, exploits and effective countermeasures.
- Provide effective countermeasures to the Best Practices Analyst.
- Produce weekly executive summaries of current vulnerabilities and exploits.
- Maintain a list of vulnerability news resources for the CSCC.

The *Forensics Analyst* position further examines and analyzes various forms of malware, exploits, phishing attempts, and related cyber-attacks. The Forensics Analyst performs certain exploits found in a developed sandbox environment. The duty requirements for this position include:
- Building and maintaining a Network Vulnerability Assessment Lab.
- Obtaining samples of viruses, malware, and phishing-attempts for analysis.
- Produce weekly executive summaries of current threats, phishing-attempts, and malware campaigns.
- Produce analysis reports of malware samples and phishing attempts.
- Publish malware remediation procedures to CSCC.

The *Industrial Control Systems Cybersecurity Analyst* further specifically examines and analyzes current cybersecurity threats related to both ICS and critical infrastructure protection. The duty requirements for this position include:

- Building and maintaining Network Vulnerability Assessment Lab equipment specifically related to ICS.
- Produce weekly executive summaries relating to ICS cybersecurity.
- Publish ICS alerts and advisories.
- Maintain ICS training and resources for the CSCC.

CSCC Portal (Available from www.uhwo.hawaii.edu/cyber)

The expansion of the CSCC Portal allows access to all analyst resources to the public to support education and the increased cybersecurity posture of networks local and regionally. The portal also support academics, training, events, jobs, internships, and cybersecurity resources (see figures 1 and 2).
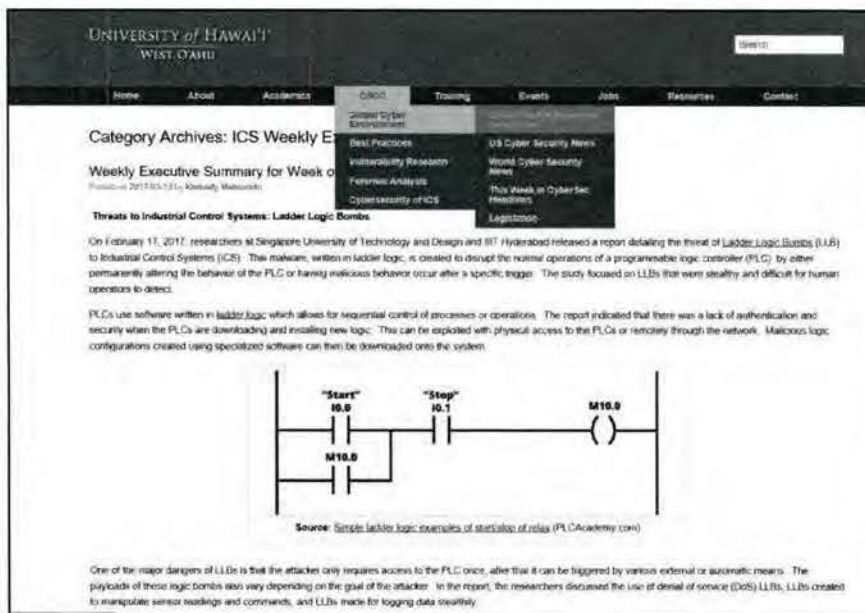
Figure 1: CSCC Portal

Figure 2: CSCC Portal

CSCC Center – UHWO Campus Room E205

The expansion of the CSCC into expanded physical space provides five student interns the resources to conduct cybersecurity research and analysis. The CSCC is configured with analyst workstations, forensics machines, and vulnerability testing platforms (see figure 3).

Figure 3: Physical CSCC

Establishment of the UHWO CSCC Network Vulnerability Assessment Lab

Ethical and legal considerations are a significant challenge when educating BAS-ISA students on techniques and procedures involved in conducting vulnerability assessments of computer networks. To adequately exercise and experiment with industry standard software, it was necessary to construct a Network Vulnerability Assessment Lab to mitigate the risks associated with conducting penetration testing on live networks. In addition, a reconfigurable lab allows students to model various network architectures and support research into the vulnerabilities associated with home networks, small business networks, and industrial control systems. Curriculum courses that support this lab include Proactive System Security, Digital Forensics, Management of Information Security, Secure Software Programming, and Senior Project. A new course was developed and offered for the spring 2017 semester to better train and educate students on the cybersecurity concerns of the Nation's critical infrastructure; Cybersecurity of Supervisory Control and Data Acquisition (SCADA) Systems.

Establishment of this lab included associated hardware and software for the on-campus lab, faculty and researcher training, administrative stipends for practicum and research students, and limited travel for site visits and conferencing.

Triangle Micro Works Test Harness: UHWO completed the purchase and configuration of network simulation and industry commercial-of- the-shelf (COTS) solution to begin understanding protocol parsing and vulnerability analysis for protocols used in critical infrastructure. The purpose of this vulnerably analysis was to gain a better understanding of information security as it applies to the protection of critical infrastructure. This will be the first test conducted in the Protection of Critical Infrastructure lab to better understand issues involved

7

in the specific protocols. This objective of this study was to implement a small-scale simulation of a utility industrial control system using the Triangle Micro Works Test Harness. Protocols involved in this test include DNP3. The simulation was used to monitor communications from a remote user to the remote terminal unit (RTU). This laid the groundwork for possible expansion of this study to include vulnerability testing of the communications to an RTU using commercial products.

NETLAB: UHWO implemented a system created by Network Development Group (NDG) called NETLAB. This system allows students to connect to a self-enclosed virtualized network environment at any time. NETLAB utilizes a virtual network called "pods" that are non-persistent and reusable for hands-on learning. The pods contain their own network and are unable to access anything outside of the environment allowing students to work safely on system penetration techniques, malware analyzing and forensics analysis. In addition, the reconfigurable lab allows students to model various network architectures and support research into the vulnerabilities associated with home networks, small business networks, and industrial control systems. Curriculum courses that support this lab include Proactive System Security, Digital Forensics, Management of Information Security, Secure Software Programming, and Senior Project and Cybersecurity of SCADA. Student interns were provided the opportunity to assist in the installation, configuration, and maintenance of the NETLAB system (see figure 4).

Figure 4: NETLAB Installation

Student Client Workstations and Lab: UHWO completed the purchase and configuration of a commercial-of- the-shelf (COTS) solution for a student lab to access penetration testing resources. This lab includes 30 workstations configured for access to the NETLAB infrastructure, host-based virtual machine penetration testing, and academic software for course support.

Expansion of the Troops to Engineers Program

The Troops to Engineers Program promotes success in engineering through internships and work experience for recent veterans. This National Science Foundation sponsored initiative at San Diego State University demonstrated a methodology to bridge the gap between military service and the transition into engineering careers. O'ahu is home to several military installations, and as of November 2010, the number of veterans in the State of Hawaii was 117, 254. The expansion of the program to UHWO allowed the university to support veterans transitioning into engineering career fields, specifically information assurance and cyber security (See Appendix B). Additionally, UHWO developed a partnership with the SPAWAR Systems Center Pacific and has a student veteran serving as an intern at the Hawaii facility.

SPAWAR Systems Center Pacific: UHWO established partnerships with SPAWAR Systems Center Pacific, Cybersecurity Science and Technology Branch. This partnership led to the support of ICS Cybersecurity training for UHWO students in support of cyber workforce development. To support this partnership, a new course was developed and offered to advanced cybersecurity students (available Spring 2017 semester). ICS cybersecurity training and workforce development are also directly supported with SPAWAR SSC subject matter experts providing student training and faculty development (see Figure 5).

Figure 5: SPAWAR Systems Center Partnership

Tasks and Timeline

The Cyber Security Workforce Development and the Protection of Critical Infrastructure Project original period of performance was from May 15th, 2015 through December 2016. This project directly supports cyber workforce development needs. The level two and three tasks from the project work breakdown structure (WBS) and associated milestones are as follows:

* Identifies a project milestone

1. Initiation	May 2015-August 2015
1.1. Stakeholder identification	5/15-6/15
1.2. Stakeholder register completed*	7/15
1.3. Stakeholder management strategy completed*	8/15
1.4. Development of white-paper*	Complete
1.5. Completion of project proposal*	2/15

2. Planning	May 2015-August 2015
2.1. Scope statement	5/15-6/15
2.2. Schedule	7/15
2.3. Initial project management plan (PMP)*	7/15
2.4. Gantt chart*	7/15
2.5. PMP*	8/15
2.6. Updated resources register with financial overhead	8/15

3. Cyber Security Coordination Center (CSCC)	Aug.2015 – Dec. 2016
3.1. Expansion of web-based coordination site	6/15-6/16
3.2. Hardware equipment plan	8/15
3.3. Hardware procurement*	8/15-12/15
3.4. Software plan	8/15
3.5. Software, licenses, and procurement*	8/15-12/15
3.6. Facilities improvement*	8/15-12/15
3.7. Communications plan and products	8/15-12/15
3.8. Travel plan	9/15
3.9. CSCC transition to sustained operations*	8/16

4. Network Vulnerability Assessment Lab	Aug. 2015 – Dec 2016
4.1. Lab design*	9/15-12/15
4.2. Hardware equipment plan	9/15-12/15
4.3. Hardware procurement*	1/15-12/16
4.4. Software plan	9/15-12/15
4.5. Software, licenses, and procurement*	1/15-3/16
4.6. Facilities improvement*	1/15-12/16
4.7. Researcher training, SCADA and penetration testing	8/15-12/16
4.8. Travel plan	8/15-12/16
4.9. Lab transition to sustained operations*	12/16

5. Troops to Engineers Program	Aug. 2015-Dec. 2016
5.1. Communication	8/15-3/16

5.2. Planning for veteran stipends	8/15-12/15
5.3. Travel plan	8/15-12/16
5.4. Support plan for CSCC*	1/16-12/16
5.5. Support plan for Network Vulnerability Assessment Lab*	1/16-12/16
5.6. Internships complete*	12/16

6. Monitoring and Controlling   Aug. 2015 – Dec 2016

6.1. Lab direction	8/15 – 12/16
6.2. CSCC operations	8/15-12/16
6.3. Stakeholder update/visit 1QFY16*	11/15
6.4. Stakeholder update/visit 3QFY16*	5/16
6.5. Final stakeholder update/visit complete*	12/16

7. Closing

7.1. Final project report complete*	3/17
7.2. Project complete*	3/17

Key Project End Items

CSCC Equipment and Supplies and Related Expenses

CSCC Hardware
> Dell Workstations
> Cyber Center laptops
> Cyber Center Display Panels

CSCC Software
> Nessus Vulnerability Scanner
> Office Software
> Deepfreeze security Software

CSCC Book Library
> Industry and academic standard texts
> CHFI Courseware
> CEH Courseware

Vulnerability Assessment Lab and Server Equipment

Lab Hardware
> NETLAB Server and associated networking equipment
> Dell Servers and virtual network equipment

Student client workstations

Lab Software
> NETLAB Installation and Training
> vSphere ESXI software for network virtualization
> Triangle Microworks Test Harness

Summary

This Cyber Security Workforce Development and the Protection of Critical Infrastructure Project directly supports workforce development needs for the U.S. Navy; promotes local, regional, and global needs to develop subject matter experts in information security and assurance; and supports the transition of veterans into engineering related career fields. The project was completed along three lines of effort: expansion of the UHWO Cyber Security Coordination Center (UHWO CSCC), establishment of the UHWO CSCC Network Vulnerability Assessment Lab, and the Expansion of the Troops to Engineers Program. The project was completed on December 31st, 2016 following the no cost extension identified in Appendix A (No Cost Extension). The estimated and final cost for the program was $360,275.

Project Highlights Include:

- UHWO Certification by the NSA and DHS as a National Center of Academic Excellence in Cyber Defense Education through Academic Year 2021.

- UHWO Team was the first in the state to win the National Cyber League, National Championship. The team placed first in both the overall and gold brackets earning the title of National Champions in 2016.

- Expansion of both the physical and virtual CSCC at UHWO supporting student research.

- Design and installation of server and client infrastructure to support cyber workforce development.

- Established Partnerships with SPAWAR Systems Center Pacific.

References

University of Hawaii West Oahu, "About UHWO," University of Hawaii West Oahu. [Online]. Available: http://www.uhwo.hawaii.edu/about-us/. [Accessed 17 12 2014].

Department of the Navy, "CNO's Position Report," Washington D.C., 2014.

National Security Agency, Central Security Service, "National Centers of Academic Excellence in Information Assurance (IA)/Cyber Defense (CD)," 2014. [Online]. Available: https://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml. [Accessed 15 12 2014].

NETLAB Product Overview | NDG. (n.d.) [Online]. Available: https://www.netdevgroup.com/products/ [Accessed 01 12 2016].

Quemado, M., Developing the Cyber Security Coordination Center (Working paper) Hawaii, (2015).

Chang, E., Cyber Security Coordination Center (Working paper) Hawaii, (2015).

Info for Veterans - Troops to Engineers | SDSU." Info for Veterans - Troops to Engineers | SDSU. [Online]. Available: http://newscenter.sdsu.edu/engineering/info_for_veterans.aspx. [Accessed 01 12 2016].

Appendix A – No Cost Extension to December 31st, 2017

UNIVERSITY
of HAWAI'I
WEST O'AHU

40 years
1976-2016

Office of the Vice Chancellor for Academic Affairs

July 15, 2016

Dr. Richard Carlin
ONR SEA WARFARE & WEAPONS S&T DEPT
875 N. Randolph Street
Arlington, VA 22203-1995

RE: Award No. N00014-15-1-2407
        No Cost Extension until December 31, 2016

Dear Dr. Carlin,

We respectfully request a No Cost Extension until December 31, 2016 for award No. N00014-15-1-2407 *Cyber Security Workforce Development and the Protection of Critical Infrastructure*. The current end date is August 14, 2016. We anticipate having a balance of approximately $104,035 left of the original award.

We request a no cost extension to facilitate the completion of projected procurement actions and scheduled student research internships. The period of performance on the grant proposal and the grant award document is from May 15th, 2015 – August 14th, 2016; however, project funding was initiated on July 28th, 2015. The additional time will also allow the project manager to continue support of the UHWO Cyber Coordination Training Center and associated student research for the Fall 2016 semester.

Thank you for your support of the program.

Respectfully,

Matthew A. Chapman, Ph.D.
Principal Investigator

Melody Bentz
Contracts and Grants Specialist
Office of Research Services

mc:sm

91-1001 Farrington Highway
Kapolei, Hawaii 96707
Telephone:(808) 689-2300
An Equal Opportunity/Affirmative Action Institution

AWARD/ MODIFICATION

3a. ISSUED BY:	Office of Naval Research 300 Fifth Avenue Suite 710 Seattle WA 98104

1. INSTRUMENT TYPE: Grant Award	3b. CFDA: 12.300
2. AUTHORITY: 10 USC 2358 and 31 USC 6304, as amended	3c. DUNS NUMBER: 195737551

4. AWARD NO.: N00014-15-1-2407	5. MODIFICATION NO.: A00001	6. MODIFICATION TYPE: ADM	7. PR NO.: 4720000527

8. ACTIVITY/AGENCY PROPOSAL NO.: GRANT11858219	9. RECIPIENT PROPOSAL NO.:	10. PROPOSAL DATE: 03/05/2015	11. ACTIVITY TYPE: R&D	12. PROGRAM TYPE: ONR

13. ISSUED TO	13b. CAGE: 38KX7	13c. EDI/EFT NUMBER: N/A	14. REMITTANCE ADDRESS (IF DIFFERENT FROM BLOCK 13):
13a. ADDRESS:			Same as Block # 13

UNIVERSITY OF HAWAII SYSTEMS
UNIVERSITY OF HAWAII - WEST OAHU
96-129 ALA IKE
PEARL CITY HI 96782-3626
UNITED STATES OF AMERICA

13d. BUSINESS OFFICE CONTACT:
Melody Bentz

13e. TELEPHONE NUMBER: 808-956-7800 **13f. EMAIL ADDRESS:** mbentz@hawaii.edu

15. RESEARCH TITLE AND/OR DESCRIPTION OF PROJECT AND/OR PROPOSAL TITLE:
Cyber Security Workforce Development and the Protection of Critical Infrastructure

16. FUNDING	ACTIVITY/AGENCY SHARE	RECIPIENT SHARE	TOTAL	17. CURRENT FUNDING PERIOD
PREVIOUSLY OBLIGATED			$360,275.00	N/A THROUGH N/A
OBLIGATED BY THIS ACTION:			$0.00	
TOTAL OBLIGATED ON AWARD:			$360,275.00	**18. PERIOD OF PERFORMANCE**
FUTURE FUNDING:			$0.00	05/15/2015 THROUGH 12/31/2016
GRANT TOTAL:			$360,275.00	

19. ACCOUNTING AND APPROPRIATION DATA:
See Attached Financial Accounting Data Sheet(s)

20a. PRINCIPAL INVESTIGATOR/RECIPIENT TECHNICAL REPRESENTATIVE:	21. TECHNICAL REPRESENTATIVE		21b. CODE: 33
Matthew Chapman	21a. NAME: RICHARD CARLIN		
	21c. ADDRESS: ONR SEA WARFARE & WEAPONS S&T DEPT 875 N. Randolph Street Arlington VA 22203-1995		

20b. TELEPHONE NUMBER: 808-689-2333	20c. EMAIL ADDRESS: schapman@hawaii.edu	21d. TELEPHONE NUMBER: 7036965075	21e. EMAIL ADDRESS: RICHARD.CARLIN1@NAVY.MIL

22. AWARDING OFFICE CONTACT		22b. CODE: BD247	23a. ADMINISTRATIVE OFFICE		23b. CODE: N63374
22a. NAME: DANIEL B DOWNER			ONR REG Office Seattle Telephone 206-548-7234 300 Fifth Avenue Suite 710 SEATTLE WA 98104		
22c. ADDRESS: Office of Naval Research 300 Fifth Avenue Suite 710 Seattle WA 98104					

22d. TELEPHONE NUMBER: 206-548-7239	22e. EMAIL ADDRESS: DANIEL.DOWNER@NAVY.MIL				

24. SUBMIT PAYMENT REQUEST TO:	25a. PAYING OFFICE	25b. CODE: HQ0339	26a. PATENT OFFICE:	26b. CODE: N00014
Same as block 23c	DFAS-CO/WEST ENTITLEMENT OPERATIONS HQ0339 PO BOX 182381 COLUMBUS OH 43218		Office of Naval Research ATTN: ONR BDCC One Liberty Center 875 North Randolph Street, Suite 1425 Arlington, VA 22203-1995	

ONR AWARD FORM (0800 - version 1.1

Appendix B- Troops to Engineers Report

Troops to Engineers Program Trip Report: Ms. Sherry Proper, Director of Strategic Initiatives

Coordination meetings with the Veterans Centers at California State University San Marcos (CSU San Marcos) were conducted on July 15, 2016 and with San Diego State University (SDSU) on July 18, 2016. The purpose of these trips was to gain a better understanding of the infrastructure of the centers, as well as their scope and services, in order to begin to devise a plan for providing similar services at the University of Hawaii West Oahu.

At CSU San Marcos, Ms. Proper met with the following representatives: Patricia Reilly, Veterans Center Director; Ericka Korb, ESTEP Coordinator and Professional Development; and Brian Pierce, ESTEP Management Intern. At SDSU, meeting occurred with the following representatives: Todd Kennedy, Veterans Coordinator; Ryan Morris, Vocational Rehabilitation Coordinator; Jason Smith, Veterans Employment Specialist; and Holly Shaffner, Military Liaison Officer.

At each of these institutions, the percentage of military-related students – including veterans, activity duty, and family members – is approximately 10-12% of the total student population. Both CSU San Marcos and SDSU are institutions that have demonstrated appreciation and support of veterans by dedicating facilities, staff and financial support to ensure veterans, active military and their family members are successful in transitioning from military to non-military life.

The mission of the Centers focusses on five key areas: family, finances, health, education, and career. Specific center services include assistance with admission and application information, educational benefits, scholarships, disability compensation claims, degree evaluation, internship opportunities, counseling, and vocational advising. According to staff members at both schools, it is workforce development and career preparation that are the most strategic components of the Centers' activities. Programs like ESTEP, VetSuccess, Troops to College, and Troops to Engineers further establish and organize specific pathways to educational and career achievement.

In order for the University of Hawaii West Oahu to begin to build the groundwork for supporting military-related families, the initial step would be to hire a staff who has knowledge of and experience in the five key areas of military support member to establish the foundation of a military-related support center. The University of Hawaii West Oahu already has some select academic programs that are attractive and conducive to military students, as well as its first ESTEP student intern. Should funding be available to lead the development of a 3-5 year pilot program, specific goals for enrollment and retention could be determined in an effort to project tuition revenue that would support the institutionalization of these efforts. Another trip to CSU San Marcos in a few months would be appropriate to have a more detailed meeting with the Veterans Financial Aid specialist there, since finances are a key area of support focus for military students and UH West Oahu needs more information about that particular area in order to establish a Veterans Center.

Appendix C – CSCC Library Inventory

(Available from http://www.uhwo.hawaii.edu/cyber/resources/uhwo-cscc-library/)

UHWO CSCC Library

The titles below are available for student reading and research in the UHWO CSCC, E205. These reference materials cannot be removed from the CSCC.

Title	Author	ISBN
A Nation Rising: Hawaiian Movements for Life, Land and Sovereignty	Noelani Goodyear-Ka'opua, Ikaika Hussey and Erin Kahunawaika'ala Wright	9780822356950
All-In-One CompTIA Security+ Exam SY0-401 Exam Guide 4th Edition	WM Arthur Conklin and Gregory White	9780071841245
Android Hacker's Handbook	Joshua J. Drake, Pau Oliva Fora, Zach Lanier, COllin Mulliner, Stephen A. Ridley and Georg Wicherski	9781118608647
Applied Cyber Security and the Smart Grid	Eric D. Knapp	9781597499989
Applied Network Security Monitoring	Chris Sanders and Jason Smith	9780124172081
Black Hat Python: Python Programming for Hackers and Pentesters	Justin Seitz	9781593275907
Blue Team Handbook: Incident Response Edition	Don Murdoch	9781500734756
Building an Information Security Awareness Program	Bill Gamer and Valerie Thomas	9780124199675
Building Virtual Pentesting Labs for Advance Penetration Testing	Kevin Cardwell	9781783284771
CCENT/CCNA ICND1 100-105 Official Cert Guide	Wendell Odom	9781587205804
CCNA Routing and Switching ICND2 200-105	Wendell Odom	9781587205798
CHFI Computer Hacking Forensic Investigator Certification All-In-One Exam Guide	Charles L. Brooks	9780071831567
CISSP Study Guide Third Edition	Eric Conrad, Seth Misenar, Joshua Feldman	9780128024379
CISSP: Certified Information Systems Security Professional Official Study Guide	James Michael Stewart	9781119042716
CompTIA Security+ Get Certified Get Ahead SY0-401 Study Guide	Darril Gibson	9781939136022
Counter Hack Reloaded	Ed Skoudis	9780131481046
Crafting the InfoSec Playbook	Jeff Bollinger	9781491949405
Cyber Warfare, Second Edition: Techniques, Tactics and Tools for Security Practitioners	Jason Andress, Steve Winterfeld	9780124166721
Digital Forensics For Legal Professionals	Larry E. Daniel, Lars E. Daniel	9781597496438
Ethical Hacking and Countermeasures v9 – Volume 1	EC-Council	N/A
Ethical Hacking and Countermeasures v9 – Volume 2	EC-Council	N/A
Ethical Hacking and Countermeasures v9 – Volume 3	EC-Council	N/A
Fuzzing: Brute Force Vulnerability Discovery	Michael Sutton, Adam Greene, Pedram Amini	9780321446114
Go! with Microsoft Office 2013 Volume 1	Shelley Gaskin, Alicia Vargas and Carolyn McLellan	9780133142662
Google Hacking for Penetration Testers	Johnny Long	9780128029640

Guide to Computer Forensics and Investigations	Bill Nelson, Amelia Phillips, Christopher Steuart	9781285060033
Hacking Exposed 7: Network Security Secrets & Solutions	Stuart McClure, Joel Scambray and George Kurtz	9780071780285
Hacking Web Apps: Detecting and Preventing Web Application Security Problems	Mike Shema	9781597499514
Hacking: The Art of Exploitation	Jon Erickson	9781593271442
Handbook of SCADA/Control Systems Security	Robert Radvanovsky	9781466502260
Hands-On Ethical Hacking and Network Defense	Michael T. Simpson, Kent Backman, James E. Corley	9781133935612
Industrial Network Security	Eric D. Knapp	9780124201149
Industrial Process Automation Systems: Design and Implementation	B.R. Methta	9780128009390
iOS Hacker's Handbook	Charlie Miller, Dionysus Blazakis, Dino Dai Zovi, Stefan Esser, Vincenzo Iozzo and Ralf-Phillip Weinmann	9781118204122
Java Software Solutions: Foundations of Program Design 8th Edition	John Lewis and William Loftus	9780133594959
Kali Linux Network Scanning Cookbook	Justin Hutchens	9781783982141
Kali Linux Wireless Penetration Testing	Vivek Ramachandran	9781783280414
Mastering Kali Linux for Advanced Penetration Testing	Robert W. Beggs	9781782163121
Mastering Windows Server 2012 R2	Mark Minasi, Kevin Greene, Christian Booth, Robert Butler, JOhn McCabe, Robert Panek, Michael Rice and Stefan Roth	9781118289426
Metasploit: The Penetration Tester's Guide	David Kennedy	9781593272883
Microsoft Office 2010 Volume 1 2nd Edition	Robert T. Gauer, Mary Anne Poatsy, Keith Mulbery, Michelle Hulett, Cynthia Krebs and Keith Mast	9780132873604
Microsoft Office Access 2010 Comprehensive	Robert T. Gauer, Keith Mast and Mary Anne Poatsy	9780135098257
Microsoft Office Excel 2010 Comprehensive	Robert T. Grauer, Keith Mulbery and Mary Anne Poatsy	9780135098592
Mike Meyer's Certification Passport: CompTIA Security+ Exam SY0-401 4th Edition	Dawn Dunkerley and T.J. Samuelle	9780071832144
Network Intrusion Analysis	Joe Fichera and Steven Bolt	9781597499620
Nmap 6 Cookbook: The Fat Free Guide to Network Scanning	Nicholas Marsh	9781507781388
Nmap Network Scanning	Gordon Lyon	9780979958717
Open Source Intelligence Techniques 4th Edition	Michael Bazzell	9781508636335
Penetration Tester's Open Source Toolkit	Jeremy Faircloth	9781597496278
Penetration Testing: A Hands-On Introduction to Hacking	Georgia Weidman	9781593275648
Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software	Michael Sikorski and Andrew Honig	9781593272906
Practice Exams CompTIA Security +	Daniel Lachance and Glen E. Clarke	9780071833448

Professional Penetration Testing	Thomas Wilhelm	9781597499934
Red Team Field Manual	Ben Clark	9781494295509
Research Design: Qualitative, Quantitative and Mixed Methods Approaches	John W. Creswell	9781452226101
Reversing: Secrets of Reverse Engineering	Eldad Eilam	9780764574818
Revised Information Technology Project Management 7th Edition	Kathy Schwalbe	9781285847092
Security Awareness: Applying Practical Security in Your World	Mark Ciampa	9781111644185
Security in Computing 5th Edition	Charles P. Pfleeger	9780134085043
Software Engineering 6th Edition	Ian Sommerville	020139815X
Stealing the Network: How to Own a Continent	Ryan Russell	9781931836050
Stealing the Network: How to Own the Box	Ryan Russell	9781931836876
The Hacker Playbook 2	Peter Kim	9781512214567
The Mobile Application Hacker's Handbook	Dominic Chell, Tyrone Erasmus, Shaun Colley and Ollie Whitehouse	9781118958506
The Network Security Test Lab: A Step-by-Step Guide	Michael Gregg	9781118987056
The Shellcoder's Handbook 2nd Edition	Chris Anley, John Heasman, Felix "FX" Lindner and Gerardo Richarte	9780470080238
The Web Application Hacker's Handbook 2nd Edition	Dafydd Stuttard and Marcus Pinto	9781118026472
Threat Modeling: Designing for Security	Adam Shostack	9781118809990
Unix and Linux Systems Administration Handbook 4th Edition	Evi Nemeth, Garth Snyder, Trent R. Hein and Ben Whaley	9780131480056
Violent Python: A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers	TJ O'Connor	9781597499576
Virtualization Security	Dave Shackleford	9781118288122
Windows Forensics Analysis Toolkit	Harlan Carvey	9780124171572
Wireshark Network Analysis – The Offical Wireshark Certified Network Analyst Study Guide	Laura Chappell	9781893939943
Your Career How to Make it Happen 8th Edition	Lauri Harwood	9781111572310