AFRL-RI-RS-TR-2018-072

COLLEGIATE CYBER DEFENSE COMPETITION EFFORT

UNIVERSITY OF TEXAS AT SAN ANTONIO

MARCH 2018

FINAL TECHNICAL REPORT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

STINFO COPY

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE

■ **AIR FORCE MATERIEL COMMAND** ■ **UNITED STATES AIR FORCE** ■ **ROME, NY 13441**

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09. This report is available to the general public, including foreign nations. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RI-RS-TR-2018-072 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE CHIEF ENGINEER:

/ S /	**/ S /**
JENNIFER A. CASSETTI	WARREN H. DEBANY, JR
Work Unit Manager	Technical Advisor, Information Exploitation and Operations Division Information Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government’s approval or disapproval of its ideas or findings.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

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 this 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)*
MARCH 2018

2. REPORT TYPE
FINAL TECHNICAL REPORT

3. DATES COVERED *(From - To)*
JAN 2012 – SEP 2017

4. TITLE AND SUBTITLE
COLLEGIATE CYBER DEFENSE COMPETITION EFFORT

5a. CONTRACT NUMBER
FA8750-12-2-0100

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Dwayne Williams

5d. PROJECT NUMBER
HS47

5e. TASK NUMBER
UT

5f. WORK UNIT NUMBER
EX

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
University of Texas at San Antonio (UTSA)
One UTSA Circle
San Antonio, TX 78249

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory/RIGA
525 Brooks Road
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/RI

11. SPONSOR/MONITOR'S REPORT NUMBER
AFRL-RI-RS-TR-2018-072

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited. This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This report serves as the final technical report for the Collegiate Cyber Defense Competition (CCDC) effort performed under grant FA8750-12-2-0100. Under this effort, the Center for Infrastructure Assurance and Security (CIAS) expanded the CCDC to a national level event and developed training materials for use in the CyberPatriot competition.

15. SUBJECT TERMS

college cyber competition national virtual training, CyberPatriot, CCDC

16. SECURITY CLASSIFICATION OF:

a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**	**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
U	U	U	UU	14	**JENNIFER A. CASSETTI**

19b. TELEPHONE NUMBER (*Include area code*)
N/A

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 SUMMARY

This effort was focused on three primary objectives: enable development and expansion of the Collegiate Cyber Defense Competition (CCDC) program, develop training materials for the CyberPatriot program, and provide an opportunity to test/showcase other Department of Homeland Security Science and Technology (DHS S&T) funded technologies. Each of these objectives was met during this effort. The CCDC program grew 111% between 2012 and 2017 and now has national reach. The training materials developed for the CyberPatriot program have been used by over 90,000 middle and high school students, and a number of technologies have been successfully integrated into the National Championship CCDC event.

2 INTRODUCTION

When the CCDC program was started in 2005, it faced serious challenges. With limited funding and resources, it was difficult for the program to expand. Even though the program was recognized by academia, industry, and government for its contribution to cybersecurity workforce development, it was not able to reach schools on a national scale. During the same time frame, the CyberPatriot program was facing a related challenge. The program was expanding but was hampered by a lack of cybersecurity training and educational materials designed for a high school audience. As the Center for Infrastructure Assurance and Security (CIAS) was involved in both efforts, we were uniquely positioned to address the challenges facing both programs. The grant submission to LRBAA 11-03 outlined our approach to address these issues and was approved for funding in 2012. The funding from this grant has enabled both programs to grow into internationally recognized competition efforts with significant contributions to cybersecurity and workforce development.

3 METHODS, ASSUMPTIONS, AND PROCEDURES

3.1 The CCDC Program

The challenges facing the CCDC program were well known at the start of this effort. For the program to grow, it needed resources to develop common competition assets, such as a service scoring engine, and support regional events. Getting students to a National Championship cybersecurity event was also a challenge as many universities did not provide financial support to competing teams. Our approach to solving these challenges was to use the provided funding to:

- Support regional activities: With the funding from this grant, we were able to establish 10 CCDC regions encompassing all 50 states. Each regional was established with a Regional Director from a participating college or university in that region and funding to support their regional efforts. The Regional Directors led outreach and recruiting efforts in their region and oversaw all qualifying and regional competition activities.

- Develop common resources: This grant also allowed the CCDC program to develop common resources used through the CCDC program. A common ruleset, competition methodology, operational processes, and scoring systems were developed and refined during this effort. These common resources greatly decreased the amount of effort to organize and conduct qualifying and regional events.

- Support virtualization efforts: The regional CCDC events and the National Championship event are "physical" events - participants travel to a central location to compete. To effectively scale the competition, we knew that a virtualized qualifying competition system was needed for each region. By partnering with the Center for Systems Security and Information Assurance (CSSIA), we were able to secure a virtualization capability that supports half the CCDC regions on an annual basis.

3.2 CyberPatriot Training Materials

The CyberPatriot training materials were developed under the assumptions that each team needed a common base of cybersecurity knowledge and that team training would be either self-taught or performed by a coach. The training materials were developed as 30 to 60 minutes lessons in PowerPoint and video format. The materials were made available to registered CyberPatriot teams through the CyberPatriot website. Teams could then download and progress through the materials at their own pace.

4 RESULTS AND DISCUSSIONS

4.1 Growth of the CCDC Program

As Figure 1 shows, the number of colleges and universities competing in the CCDC program continues to grow each year thanks to the efforts supported by this grant.

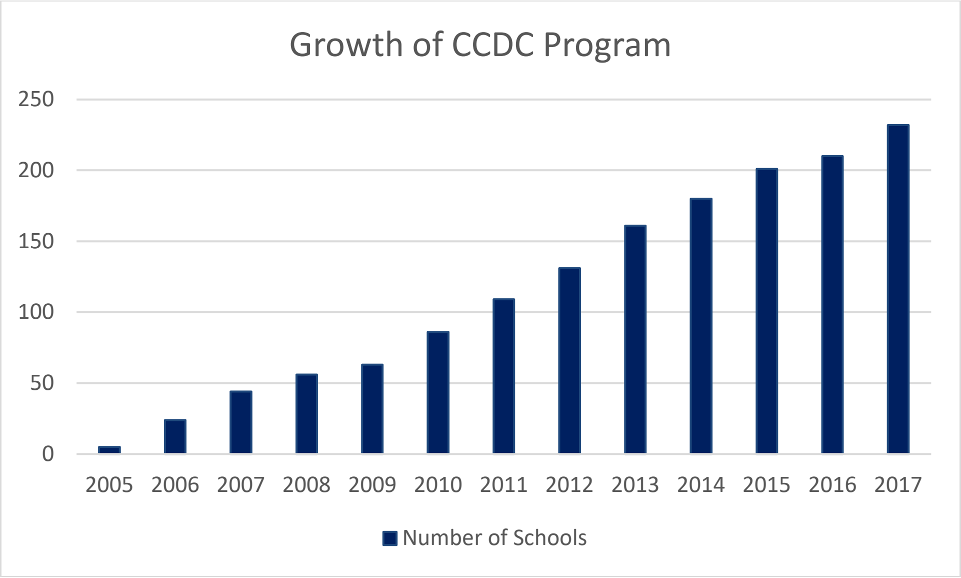

Figure 1: Growth of CCDC Program

The CCDC program has grown into a national event with participating colleges and universities from 46 of the 50 states including Alaska and Hawaii (Connecticut, Nevada, North Dakota, and Rhode Island are the only states without teams in the CCDC). With support from this grant, the CCDC has become the largest college level cyber defense competition program in the United States.

4.2 Virtualized Environments

A key factor in the growth of the CCDC program has been the use of virtual environments. Virtual environments are easier to setup and maintain than physical environments, allow for rapid reuse and redeployment, and are more easily accessible to remote participants. To enable participation for more teams, the CCDC program uses virtual qualifiers where every competing team meets in a virtual arena. The CIAS worked closely with CSSIA at Moraine Valley Community College to develop a virtual arena capable of supporting CCDC events. CSSIA, who also hosts the Midwest CCDC Region, continues to provide virtual qualifier support to their local state competitions as well as other CCDC regions.

Virtualized environments also allow participation from geographically remote schools – such as those in Alaska and Hawaii. While most CCDC regions employ a virtual qualifier / physical regional event model, the costs associated with traveling to a physical regional event for schools in Hawaii and Alaska were prohibitive. The creation of the all virtual At Large CCDC region has allowed schools from remote areas to participate in CCDC events.

4.3 NCCDC Competition Environments

Another key factor in the growth and success of the CCDC program has been the use of realistic small business environments in the competition. At each level of the CCDC program, competitors are given identical, operational small business environments complete with users, files, critical services, and so on. Each year a different small business sector is chosen for the National Championship network, and significant effort is expended to create a competition network that mirrors a small business operating in that sector. The competition environments for the National Collegiate Cyber Defense Competition (NCCDC) for 2012 through 2017 were:

- 2012: Go-Mommy – an Internet domain name and website hosting company.

- 2013: The Jamestown Correctional Institute – a prison system.

- 2014: Warp Core Gaming – an Internet game hosting provider.

- 2015: Stark Energy – an electrical utility company.

- 2016: ODIN Security – a small aerospace and defense contracting firm

- 2017: Dwarven Hammer – a comic book and collectibles retailer.

4.4 DHS S&T Sponsored Projects

At the beginning of this grant effort, DHS S&T and the CIAS came to the joint conclusion that CCDC environments could serve as ideal testing grounds for other DHS S&T sponsored efforts. CCDC environments try to create a realistic small business environment for each competition but do so in a completely controlled environment. Testing products in this type of “no risk” environment provides great results. CCDC environments are more robust and detailed than most test or development environments, involve more systems and users than test/development environments, and provide “production environment” test conditions without endangering actual production environments. Beginning in 2013, a variety of DHS S&T sponsored technologies were integrated into the NCCDC environments.

During the 2013 NCCDC, a team from the Pacific Northwest National Laboratory brought their Traffic Circle program to San Antonio to test it in a traffic-intense, near real-world environment. Traffic Circle provides a visual representation of network traffic. The sheer volume and complexity of the NCCDC traffic allowed Traffic Circle engineers to perform traffic testing they had previously been unable to perform. The insight gained from their experience at NCCDC, allowed the Traffic Circle engineers to highlight and ultimately address several performance issues within their product. A separate team consisting of individuals from Queralt, BridgePoint, Radiant Logic, Johns Hopkins Applied Physics Laboratory (JHAPL), and DHS S&T came to San Antonio to integrate the Personal Identity Verification (PIV) card system into the 2013 NCCDC competitor and operations networks. This integration effort yielded significant lessons learned that were taken back to improve and refine the PIV card system.

In 2014, multiple DHS S&T efforts were integrated in the NCCDC environment. Competitors were required to implement and use DNSSEC to protect and validate DNS records. While DNSSEC was essentially an “off the shelf” product at that point, integration did provide competitors and faculty coaches an opportunity to work with and discover the benefits of DNSSEC firsthand. Teams were also given copies of Entrap – a DHS funded desktop security system. Entrap was provided to each of the 10 teams competing at the 2014 NCCDC. Unfortunately, only a Windows 7 client was available for use which limited the functionality of the product during the competition. Feedback was provided to the Entrap developers requesting both Linux and Windows Server compatible versions of the product. Additionally, teams were provided with a Proactive Incident Response Command Shell (PIRCS), a DHS funded forensics system. The PIRCS product integrated very well into the 2014 NCCDC. Exelis, the developer, provided on-site support and developed two different forensic scenarios that challenged the competitor's forensics skills. We received a good deal of positive feedback regarding the PIRCS product and the scenarios using PIRCS during the NCCDC. The PIRCS product performed very well for competitors during the competition and the feedback provided by the competitors allowed Exelis to refine their training materials and enhance their product. The final product integrated into the 2014 NCCDC were a more refined version of the PIV cards. The PIV cards and supporting systems were the most complex product integrated into the 2014 NCDCC environment. For the 2014 NCCDC, the Southwest Texas Regional Advisory Council (STRAC) brought their credentialing kiosks out to the NCCDC and created badges onsite for the competitors. Those badges were then registered with the local attribute system. Individual policy gateways were installed in each team's environment with a single "master" system located in the main Operations area. The idea was to have teams add records to their local Active Directory servers that would be accessed by the policy gateways and supporting systems to validate PIV cards from team members, white team members, orange team members, etc. This year JHAPL brought out a tablet-based solution with an attached reader where teams could swipe a card to test its "validity". Authorized cards would receive a green light while unauthorized cards would receive a red light. Only a single team was successful in completing all the tasks required to make the end to end validation process work. Following the NCCDC we held a short debrief with the JHAPL personnel to discuss options for simplifying future competition setups. While the technology wasn't really designed to be setup and torn down in a matter of hours as it was during NCCDC, we did see this year that it is possible for a group of people with little exposure to the systems and technologies involved to successfully implement a PIV card validation system that worked end to end – that is the system validated both local cards and card whose credentials were stored on the master Backend Attribute Exchange (BAE).

In 2015, the CIAS integrated two DHS S&T sponsored technologies. A complete scenario based on the CyberWise product from Applied Vision was developed. This scenario would challenge the competitors to develop a "Choose Your Own Adventure" (CYOA) comic using the web-based CyberWise product. The competitors were tasked to "to develop a comic that trains our employees on what they should do and how they should react when they receive a phishing email that looks like it's coming from someone inside the company." The competitor submissions were developed on-line using Applied Visions servers and grade by Applied Visions personnel. The CIAS also worked with Pacific Northwest National Labs to create a substation, control center, and plant center for a small electrical utility. The substation consisted of a "poster" wired with Light Emitting Diode (LED)s, an Arduino, and 3 Raspberry Pi devices. The 3 Raspberry Pis simulated control elements for the substation breakers, voltage regulators, and current regulators. The Arduino monitored the Raspberry Pis to provide an out of band "ground truth" status that could be used for scoring purposes. The control center network consisted of 7 virtual machines housing engineering workstations, HMI software, OPC software, network monitoring, and logging software. Each team's control center network, substation, and plant network were housed behind a Juniper firewall so that the plant network and substation were only accessible from inside that team's control center network. We were able to integrate this simulated electrical utility infrastructure in the 2015 NCCDC. Those integration efforts allowed (Pacific Northwest National Laboratories (PNNL) to refine their design and use this same infrastructure in future efforts to secure supervisory control and data acquisition (SCADA) networks.

During the 2016 NCCDC, the CIAS worked with Secure Decisions to include their updated "Comic-BEE" technology. Comic-BEE is the updated version of the Cyber-WISE choose your own adventure comic creation tool that debuted in the 2015 NCCDC. The CIAS worked with Secure Decisions to create a new scenario for the 2016 NCCDC. There were some initial challenges getting access to the Comic-Bee servers as the NCCDC uses a white listing proxy to filter competitor network traffic, but once all the servers used by Comic-Bee were identified and added to the proxy the competitors were able to access Comic-Bee without further interruption. Secure Decisions used the feedback from the students to refine their Comic-Bee product.

4.5 Log Files from NCCDC Events

Early on in this effort, DHS S&T and the CIAS realized NCCDC events create a very valuable output – network traffic logs. Unmodified network traffic logs containing live user activity, real systems, attributable IP addresses, and real attacks are extremely hard to obtain as most organizations will not provide copies of their actual network traffic to anyone. On the rare occasions traffic logs are shared, they are typically heavily modified with IP addresses changed or some traffic completely redacted. The traffic from NCCDC events is extremely valuable in that it can be used without any modification by researchers, students, or anyone else needing "real world" traffic logs.

At NCCDC events, every individual using or connecting to the network is informed that network traffic is captured and released. NCCDC operations staff sniff all traffic passing through the core switch used to interconnect the Red Team, Orange Team, Blue Teams, and scoring systems. Traffic is captured in simple TCPDUMP format and serialized into 1 GB or 500 MB segments. The average size of an entire NCCDC traffic capture varies from 1 to 1.5 TB. At the end of each NCCDC event, the capture files are uploaded to the Information Marketplace for Policy and Analysis of Cyber-risk & Trust (IMPACT) where there are made freely available to any researcher or student. The log files for the 2012 through 2017 NCCDC events are available at https://www.impactcybertrust.org/. According to IMPACT site administrators, NCCDC log files accounted for almost half of the downloads in 2016.

4.6 Regional CCDC Hosts

A key resource provided by this grant effort was funding to support each CCDC region. From the 2013 season through the 2017 season, the CIAS provided sub-awards to each of the 10 regional hosts. This funding provided for course buyouts, equipment purchases, facility rental, or any other valid expense incurred by the regions while hosting that year's CCDC events. In some parts of the country, the regional host moved from school to school on an annual basis, while in other parts of the country the same school has served as the regional host for years. The following table shows the schools hosting a CCDC regional event by year.

Table 1: CCDC Regional Hosts by Year

School	2012	2013	2014	2015	2016	2017
Cal Poly Pomona	X	X	X	X	X	X
Community College of Baltimore County	X	X	X			
Dakota State University	X	X	X	X	X	X
Highline Community College			X	X	X	X
Kennesaw State University	X	X	X	X	X	X
Moraine Valley Community College	X	X	X	X	X	X
Northeastern University	X					
Prince George's Community College				X	X	X
Regis University	X	X	X	X	X	X
Rochester Institute of Technology						X
Syracuse University				X		
Texas A&M University	X					
Texas A&M University at San Antonio		X	X	X		
University of Alaska Fairbanks	X	X	X	X	X	
University of Maine		X			X	
University of New Hampshire			X			
University of Tulsa					X	X
University of Washington	X	X				
Virginia Polytechnic Institute and State University						X

4.7 CyberPatriot Training Materials

As the final piece of this effort, the CIAS developed cybersecurity training materials suitable for use in the CyberPatriot High School Cyber Defense Competition. Working with the Air Force Association (AFA) and high school educators, the CIAS created educational materials that included lesson plans, self-paced modules, and practical exercises to educate both instructors and students. Developed materials were published for download on AFA’s CyberPatriot website and have been accessed by over 85,000 middle and high school students since their creation in 2013. Portions of the training materials have been updated annually since 2015 to maintain relevance with advances in operating systems and the cybersecurity field. Competition organizers have directly credited these training materials as a key contributing factor to the rapid growth of the CyberPatriot program.

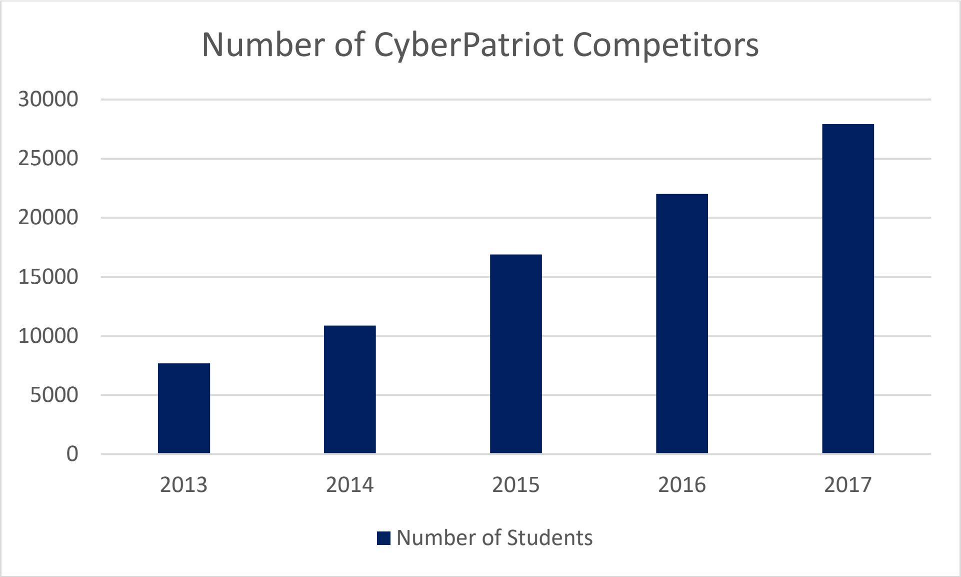

Figure 2: Growth of CyberPatriot Competitors

5 CONCLUSIONS

While not a traditional grant effort, this effort was extremely successful and produced some significant and long-lasting impacts. The funding provided by this grant has enabled the CCDC program to become one of the most respected and significant cybersecurity competitions around the world. This effort also helped the CyberPatriot competition become the largest cybersecurity competition in the world. The log files produced by the NCCDC events are used by students and researchers around the world on an almost daily basis. Both the CCDC and CyberPatriot competition efforts are helping to address the worldwide shortage of cybersecurity personnel by motivating and training future generations of cybersecurity experts.

LIST OF ACRONYMS

AFA – Air Force Association
BAE - Backend Attribute Exchange
CCDC - Collegiate Cyber Defense Competition
CIAS - Center for Infrastructure Assurance and Security
CSSIA - Center for Systems Security and Information Assurance
CYOA - Choose Your Own Adventure
DHS - S&T Department of Homeland Security Science and Technology
DNSSEC **-** Domain Name System Security Extensions
NCCDC - National Collegiate Cyber Defense Competition
IMPACT - Information Marketplace for Policy and Analysis of Cyber-risk & Trust
JHAPL – John Hopkins Applied Physics Laboratory
JHUAPL - Johns Hopkins University Applied Physics Laboratory
LED – Light Emitting Diode
PIRCS – Proactive Incident Response Command Shell
PIV - Personal Identity Verification
PNNL – Pacific Northwest National Laboratories
SCADA - Supervisory control and data acquisition
STRA - Southwest Texas Regional Advisory Council