HEADQUARTERS
CIVIL AIR PATROL
UNITED STATES AIR FORCE AUXILIARY

MEMORANDUM FOR HQ CAP/CC November 12, 2016

FROM: NATCAPWG/CC

SUBJECT: Final Report of the Civil Air Patrol Cyber Study

This is the final report for the Civil Air Patrol (CAP) Cyber Study. Overall, the study finds that CAP is making great strides in addressing current and future cyber needs in the burgeoning cyber environment. Throughout the study, the progress towards a holistic program addressing cadet and adult training and education is under development by the CAP Cyber Team.

The Cyber Study spent a great deal of time on the development of cyber-related Cadet Programs. These elements offer the greatest opportunity for CAP engagement and long term influence upon the nation's ability to address this vital issue. The Study finds that CAP should provide a holistic program for cadets that begins with a squadron-level program that provides an overview of cyber operations, hygiene, and career opportunities. CAP National Headquarters has already begun modifying their program and courseware to meet this objective.

Building upon the squadron program will be the Wing and Region Level programs which are now in its trial stages in Middle East Region. These programs will expand on the cyber programs overview at the squadron level and will provide an introduction to cyber defense technical concepts and skills. The capstone for cadet cyber programs is the Cyber Defense Training Academy which provides three levels of courses aimed at preparing cadets to take and pass certification tests like Security Plus and Network Plus.

Working with the Air Force and industry partners, provides our best opportunity to serve the needs of the Military. By helping cadets attain industry certifications prior to enlisting in the military, they will be able to shorten military recruits' training pipeline as well as decrease the number of washouts during the long training process. For industry partners, they will increase their opportunity to hire employees that can make an immediate impact for their customers, which of course includes the military. The Study recommends retention of the expanded cadet program and endorsement and support for cadet cyber security certifications.

The study evaluated numerous ongoing and proposed opportunities for CAP senior member participation in Aerospace Education, Cadet Programs and Emergency Services. Current progress by the CAP Cyber Team has successfully pushed the envelope for an inclusive program which addresses many aspects of cyber defense and engagement beyond what is generally found in organizations today. The Study endorses the continuation of these programs, beginning with the establishment of squadron, wing and region cyber officers to orchestrate the program. Further, region programs' collaboration will help to ensure that CAP cyber programs remain synchronized.

The CAP organization currently places the Cyber Team under Cadet Programs at the National Headquarters. This placement was optimum for the fledgling organization, however, as the program has matured, CAP National Headquarters should consider establishing a Division or Branch within the Operations Directorate to provide focused operations support. This would enable CAP to more fully explore opportunities in support of Emergency Services and provide greater voice for the program outside of Cadet Programs.

The most lucrative opportunity for the expansion of the program for adult members is through the widespread communication of, and opportunities for, adult members to assist in the education and training of cadets, promulgation of a spirit of cyber defense within CAP. Instilling a strong cyber ethic and ethos with the entire force will serve all our members, foster interest, and participation in, cyber-related programs, and improve personal and unit cyber security. Through this, members interested in cyber professionals will be able to impart their knowledge upon the follow adults and cadets in the aforementioned programs.

Furthermore, it is possible for CAP members to serve the corporation by providing cyber defense for CAP National Headquarters and its extended enterprise. However, network operations and cyber defense is contracted by CAP and the complexity of replacing these commercial services with volunteers are complex and expensive. These challenges include: purchase of cyber defense equipment, development of a holistic cyber defense strategy for the corporation, and operations of defensive systems through a distributed model. Again, the complexities to augmenting or replacing the current service model are significant and likely render the augmentation/replacement concept unfeasible. Conversely, cyber volunteers could be useful in assisting CAP's IT

department in a variety of operations support activities, especially in the arena of policy and cyber defense.

Recently reported Russian probing of the US Election system and a Russian-Chinese Distributed Denial of Service Attack on US Domain Name Servers (DNS) in October 2016 renewed the importance of cyber defense to the larger US Government (USG). Calls for a Cyber Civil Defense Force, possibly under the Department of Homeland Security, and an Air Force Digital Service may offer potential opportunities for CAP if either is developed beyond its current conceptual stage, operates within the unclassified environment, and if these programs are receptive to volunteer programs. Though these programs are only in a conceptual stage, CAP might make some modest investments in preparation for meeting potential requirements.

As the possible Civil Cyber Defense organizations come to being, CAP would be well positioned to provide trained volunteers to augment that cyber defense workforce. CAP vetted, well-disciplined, and Incident Command System knowledgeable force would appear a perfect match for this mission. CAP should also work with these organizations to ensure our background training and skills meet their needs. CAP should not, however, seek to train the volunteer workforce to program standards. Rather, CAP should provide the workforce and mission partner should provide that force training and certification. CAP should also not seek to provide formal cyber defense training to its adult members in support of these ends…suitable, high quality cyber defense training is available nationwide through Community Colleges, universities, and technical training centers.

The Department of Defense recently conducted a “Bug Bounty” experimental program that sought outside involvement in identifying weaknesses in the Department’s cyber defense of the Pentagon. While there may be merit to participation in such activities, CAP’s program requires significant maturation prior to participation and the Study had mixed opinions about recommending participation owing to possible risks to Civil Air Patrol’s authorities under Title 10, USC as a “noncombatant.” A formal legal option should be rendered by both CAP-USAF and CAP, and an operations review conducted prior to consideration.

After careful study and interviews with Headquarters US Air Force, US Cyber Command, and Air Force Cyber the overwhelming consensus is that there is currently no role for CAP participation with the US Air Force in its operational lines of effort within

the cyberspace mission area. Obstacles to success include a lack of access to security clearances and cyber defense weapons systems, systems training, and an ability to maintain system currency requirements. Additionally, the added complexity of inserting CAP volunteers into the Air Force's cyber operations presents "a complexity that outweighs any value opportunity the use of CAP might present."

It has been our pleasure to support the Commander and the CAP Board of Governors with this Study. Cyber Operations are critical and of increasing importance to the corporation, the US Air Force, and the nation and, therefore, warrants our attention. We recommend advancing the program as outlined and continuing to evaluate the environment for future program needs in support of cyber defense. In conclusion, Civil Air Patrol has the foundations of a strong program in support of the corporation and the nation while supporting cyber operations through education and training, promulgation of a spirit of cyber defense, and instilling a strong cyber ethic and ethos with the entire force.

Bruce Heinlein

BRUCE B. HEINLEIN, Colonel, CAP