OFFICE OF THE NATIONAL COMMANDER
NATIONAL HEADQUARTERS
CIVIL AIR PATROL
UNITED STATES AIR FORCE AUXILIARY
MAXWELL AIR FORCE BASE, ALABAMA 36112-5937

18 July 2019

MEMORANDUM FOR ALL CAP MEMBERS

FROM: CAP/CC

SUBJECT: Interim Change Letter – CAPR 120-1, *Information Technology Security,* 1 October 2017

1. Since the release of CAPR 120-1, additional security measures have been identified as necessary to enhance protection of Civil Air Patrol's information systems. The focus of these changes is centered on preventing circumvention of eServices authentication as well as added data protection requirements.

2. eServices authentication is in place to ensure system integrity by restricting access to authorized end users. Risk to our systems occurs when tools, such as automated scripting or bots, are used to logon to eServices from external systems. In doing so, members risk collection, however temporary, of their account information by these systems making unauthorized use of their account possible. Individuals who develop and provide information technology applications that employ these prohibited services place all CAP data at risk.

3. Recent international and federal data protection regulations have emphasized the need for diligence in the security of our members' data. To reduce Civil Air Patrol's jurisdictional and security risk, General Counsel and the CIO/DCIO have determined that all Civil Air Patrol data must be hosted within the continental United States.

4. This interim change letter will remain in effect until the next revision.

5. CAPR 120-1 is amended as follows.

a. Paragraph 6 Unacceptable Use. Change subparagraph 6.16. to read:

6.16. Members may not attempt to circumvent the eServices authentication or security of any account, network, or host. This will include, but is not limited to:

- accessing an account or data for which the member is not authorized outside of their eServices permissions or approved CAPWATCH dataset.
- probing the security of the networks.
- attempting an unauthorized upload or change to information in eServices.
- as a member who creates or manages local information technology, using automated scripting tools that circumvent the user's eServices logon within the local application.
- as a member who uses local applications, providing your eServices account information for use by a local application or service utilizing automated scripting tools that circumvent the eServices end user logon. When members need to access eServices applications, they must logon through the NHQ IT eServices

logon page and not through any local application or service. Local applications and/or services that logon to eServices on behalf of the member are not permitted and will not be used by members.

b. Paragraph 11 Data Security. Add subparagraph 11.8. to read:

11.8. When selecting commercial cloud services, IT Directors and IT Officers must ensure that the service is hosted inside the boundaries of the United States to avoid jurisdiction issues and concerns about inadequate security controls.

6. Please direct any questions you might have to capadmin@capnhq.gov.

Mark E Smith

MARK E. SMITH
Major General, CAP