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

30 June 2017

MEMORANDUM FOR CAP Command Council

FROM: CAP/CC

SUBJECT: CAPWATCH Process Change

1. As many of you are aware, Civil Air Patrol has embarked on an improvement effort aimed at modernizing CAP's Information Technology (IT). As part of that effort, CAP IT continuously conducts assessments to determine CAP's most urgent security risks. These reviews have consistently pointed to the high level of risk arising from the vast quantity of data that is available to, and held by, members across the country via CAPWATCH downloads. CAP leadership has little visibility into who has access to this data once it is downloaded from eServices, how it is being protected and the purpose for which it is used. Furthermore, CAP IT has been providing a customized CAPWATCH dataset to support local systems such as IMU/WMU and CAPSTAR. In addition to the data concerns I've outlined, these daily customized database pushes require maintenance efforts from the CAP IT team whenever updates are made to NHQ servers. Providing a remedy in those situations ultimately siphons capacity from our constrained IT development team and impacts their ability to complete other previously-identified high priority projects.

2. Use of these local systems also has a negative mission impact. Data can be lost when local systems are not properly maintained, and most of these local systems do not have the redundant backups and disaster recovery options in place that CAP IT does. Even worse, our personnel and units become less interoperable as they become more dependent on local systems rather than using WMIRS, Ops Quals, ORMS, and the other CAP IT tools available in eServices. In the transient society in which we live, where members may move and change units often, it is critical to standardization and their member experience that every unit use the same tools and functionality so that members can move seamlessly from one part of the country to another and continue supporting CAP.

3. After careful consideration, I have made the following decisions to mitigate the identified data risks and capacity constraints described above:

a. The current CAPWATCH delivery method will stand down on 2 January 2018. In its place, CAP IT will develop a secure subscription service within eServices that provides a standardized CAPWATCH dataset to Senior Members who are authorized by their Commander to receive it. Senior members will need to request access to this service, and as part of that request, will have to document how the data will be used. Data will be provided based on the Senior Member’s assigned organizational level. Those receiving the download will be required to sign an online user agreement that defines their responsibilities to protect the data in their care. Members and commanders will be expected to re-validate need for this data annually. The online system to support the new process will be released well in advance of the 2 January date to ease the transition from the current on-demand system to the new secure delivery system.

b. Effective on 2 January 2018, CAP IT will no longer send specialized CAPWATCH datasets to support any external system. Approved use of the limited subscription service noted above will be all that is allowed.

c. Also effective on 2 January, members are directed to discontinue using WMU/IMU, CAPSTAR, and similar locally developed mission systems. Users and administrators of these local systems will need to plan for a transition to the functionality provided within eServices prior to the end of this calendar year. Data and reports stored in these systems like sign-in logs, incident action plans, aircraft scheduling or emergency contact data, etc. should be moved into the appropriate applications in eServices before shutting them down. We suggest that you stop using these systems well before the deadline so that continued usage does not add to the data that your staff must transition.

4. I understand that these decisions change the way that we have historically distributed and used corporate data. As we mature the capabilities of CAP IT, we must adopt industry best practices to secure our systems and information. Our goal will always be to balance risk and our operational needs in ways that mitigate security concerns while allowing us to still accomplish our mission.

5. CAP IT has committed to a robust communications plan working across the staff to disseminate information about the new process and timelines well ahead of the transition. Please stand by for further communication regarding specific requirements and next steps that you will need to take as we implement the new process.

6. In closing, I ask for your assistance and support as we improve our data security. I also ask for your help in explaining to the members who serve under your command why this change is necessary. As a leader in our organization, you know that CAP takes data security very seriously and our members should expect nothing less. Thank you.

JOSEPH R. VAZQUEZ
Major General, CAP

cc:
CAP/CO/CP/DC/DO/DP/GC/IG/IT/
LG/SE/AE/FM/PD/PA
CAP-USAF/CC/CV/DO/IG/JA/LG