

## **System Security is Everybody's Job!**

A very important part every system user can play in safeguarding the security of DCPS is through good password selection and maintenance.

- Passwords should include at least one non-alpha character. Repeating, consecutive characters should not be used. Passwords should not be the name of a relative or pet, a part of your social security number, birth date, name of a sports figure or team, dictionary word, or any other easily guessed word or item that uniquely identifies the user.
- Generic passwords, initial passwords that come with new systems, or passwords provided by systems administrators should be immediately changed to a personal password.
- Passwords must be changed every 90 days. Passwords are not to be reused within 10 changes and must differ from the previous password by at least 3 characters. A different password should be used for each system you access.
- Even with all of these conditions, passwords should be easy to remember so that you do not need to write them down, but rather commit them to memory. Passwords are never to be shared.
- You should never provide your personal passwords to anyone in any manner, including over the telephone or via email. This includes technicians claiming to need your password in order to do repairs or maintenance.
- Do not leave your terminal unattended with applications open. Do not use "Hot" keys as a substitute for user IDs or passwords.
- If there is reason to believe that your password has been "compromised", take action to change the password and immediately and personally notify your TASO and/or supervisor of the circumstances.

***Following these guidelines can help keep you and the system safe!***