INTERNAL CONTROLS COMMUNIQUÉ

Div. of Military & Naval Affairs	Internal Control MNAG-IC	Bi-Monthly No. 2

In this newsletter I will be discussing a variety of internal control topics. I hope these topics act as friendly reminders and help to refresh your processes on proper internal controls.

COMMON ACCESS CARDS. You are **not** allowed to share your Common Access Card (CAC) and Personal Identification Number (PIN) with anyone. It is a serious access control violation to give your CAC and PIN to someone else to access Department of Defense computer systems. Reference your applicable service component's information systems policy on access control; AR25-2 for Army and AFI33-100 for Air Force.

Employees are responsible to keep their CAC updated. At about one month prior to your CAC expiration you should take action to renew the card:

- For State employees who do not work at an airbase, contact the State Human Resource Office before going to a Defense Eligibility Enrollment Reporting System (DEERS) location.
- For State employees who work at an Airbase contact the Security Forces unit on your base for CAC renewal before going to the DEERS location on your base.

TIME CARDS. This year I did internal control testing on a small sample of time cards. The control I tested was Human Resources' review of time cards. The outcome of the review had an unexpected result; many inaccuracies recorded on the time cards were corrected by Human Resources. While the Human Resources Time and Attendance personnel caught the errors in their review, time cards should be submitted with minimal errors. Everyone will make a mistake from time to time but blatant or numerous errors indicate that the time cards were not properly filled out and reviewed.

Please remember that the employee and supervisor's signatures mean that the time card information is **certified as correct**. All employees are expected to report accurate time cards and supervisors are responsible for reviewing time cards for accuracy.

PERSONALLY IDENTIFIABLE INFORMATION (PII). PII is any information that is identifiable to a person. The following is a list of the most common types of PII and it is not all inclusive: home address, home telephone number, personal electronic mail address, Internet identification name and password, parent's surname prior to marriage, drivers' license number, social security number, and date of birth.

All employees have the responsibility to secure PII in their work environments. All PII should be secured and safeguarded. Whether that means locking filing cabinets after office hours, password protecting folders on shared drives, or restricting access rights with on-line applications, this will prevent any intentional or unintentional use of anyone's PII. Commonly overlooked documents with PII are phone rosters, recall rosters, birthday club lists, and travel vouchers.

Any breach or complaints of a misuse of PII should be immediately reported to DMNA's Privacy Officer, Mr. Fredrick Alber at 518.786.4577.

INTERNAL CONTROL TRAINING. During the second week of July 2011 you will receive information on Internal Control training from the Human Resources Office (MNHS). Internal control training is required by The New York State Governmental Accountability, Audit and Internal Control Act of 1987. All State employees are required to take a self-study Internal Control course on-line through NYS-Learn by the Governor's Office of Employee Relations (GOER). There will be two modules, one for line-staff and another for supervisors. Stay tuned for more information to follow!

EVERYONE is responsible for internal controls!

This newsletter was written by Jennifer Winters, jennifer.winters1@us.army.mil DMNA's Internal Control Officer