



# Information Management, Technology & Reengineering and Joint Medical Information Systems

## Managers' Internal Control Program



### INFORMATION BULLETIN

Volume 4, Issue 1

December 14, 2006

#### Special Note:

One of the real joys of the Holiday Season is the opportunity to say Thank You. At the MIC Program Office, we agree and would like to say a special thanks to everyone involved with the MIC Program for all their hard work and dedication.

We would also like to extend our warmest thoughts and best wishes for a wonderful holiday and a very Happy New Year.



*"Internal controls help ensure the integrity of internal information, efficiency of operations, and compliance with laws and regulations."*

## Significant Changes to the FY 2007 Purchase Card Operating Procedures

The following contains a list of some of the significant changes in the FY 2007 Contracting Center of Excellence (CCE) Purchase Card Operating Procedures. All Billing Officials (BOs) and Cardholders (CHs) are required to comply with this guidance and should be aware of all changes implemented this year.

1. Mandatory C.A.R.E. training is now included with the CCE Orientation Training Course.
2. All CHs and BOs are now required to complete **annual** refresher training.
3. Copies of all training

certificates must be forwarded, either by fax or email, to the CCE Office to ensure the training database remains current.

4. When establishing a new purchase card account, CHs are no longer required to self-certify their credit worthiness.
5. Coming later in FY 2007, the U.S. Bank will initiate a new version of C.A.R.E. called Access On-line (AXOL). AXOL will improve system operations and allow access to 24 months of account data.
6. **The CCE Review**



**Checklist has been completely revised.**

7. Additional items have been added to the list of Restricted and Unauthorized Purchases.
8. There is a new checklist for transactions over \$2,500 up to \$25,000.
9. Jack Perry is now the agency point of contact for TMA. He may be reached at (703) 681-1143 x 5429.

For a copy of the Purchase Card Operating Procedure please visit [http://www.ha.osd.mil/mhscio/Man\\_Ctrl\\_Prog\\_Guidance.htm](http://www.ha.osd.mil/mhscio/Man_Ctrl_Prog_Guidance.htm).

## NIST Releases New Information Security Handbook for Managers

On November 7, 2006, the National Institute of Standards and Technology (NIST) released the *Information Security Handbook: A Guide for Managers*.

The handbook was designed to provide managers (agency heads, chief information officers, and other information security offi-

cial) with an overview of the information security program elements and assist them in understanding the federal government's information security program.

This handbook provides guidance that will facilitate a more consistent approach to information security

programs across the federal government.

For a copy of the Information Security Handbook please visit [http://www.ha.osd.mil/mhscio/doc\\_library.htm](http://www.ha.osd.mil/mhscio/doc_library.htm)



## Top 10 Purchase Card Weaknesses for FY 2006



The Contracting Center of Excellence (CCE) Office has identified the following as the most common findings from their FY 2006 Billing Official Reviews. (In parentheses is the percentage of accounts that had the particular finding.)

1. Late payment certification. (48%)
2. Credit limits exceed procurement needs. (47%)
3. C.A.R.E. Transaction Log not maintained. (32%)
4. Repeat findings from FY 2005 review. (31%)
5. Independent receipt and acceptance not documented. (27%)
6. Mandatory source violations. (23%)
7. Training certificates missing or training overdue. (19%)
8. Legitimate government need missing or inadequate. (18%)
9. Billing official annual review missing or inadequate. (16%)
10. Alternate billing official not designated. (13%)

**Billing Officials should specifically note these problem areas when conducting their annual reviews.**

*Source: CCE Purchase Card News, September 2006*

## Don't Take the Bait, the Control is in Your Hands

One of the hottest scams on the internet today is called Phishing. Phishing is essentially an online con game run by tech-savvy con artists, also known as phishers. Phishers send out fake emails or pop-up messages trying to trick people into sending them their personal information. These messages then direct you to a website that appears to be from a reputable business, organization, or federal agency.



of an organization posing as a colleague or company executive in an effort to steal passwords and other sensitive information. Some messages may even prompt users to open-up an attachment or click a hyperlink that will in turn download spyware, "Trojans", or other malicious software programs that will allow phishers to gain access to the company's network and files.



Another form of phishing that's wreaking havoc on businesses and government agencies alike is spear phishing. Spear phishing is a more targeted approach to phishing that involves attacks on large companies versus individuals. In this case, spear phishers send messages to members

Phishers are able to create messages and websites that look very authentic. They can duplicate logos and email addresses so that these messages and websites look legit, but **don't take the bait**. Hundreds of thousands of people are lured in by phishers each year, but with increased awareness and safe practice we can all help prevent future attacks.

Here are a couple tips on "How not to get hooked by a Phishing Scam."



1. Don't respond to email or pop-up messages asking for personal information.
2. Don't provide personal information over the internet unless you are using a secure site.
3. Don't open email attachments or hyperlinks from unknown sources.
4. Forward suspicious emails to the HA/TMA Network ([spam@tma.osd.mil](mailto:spam@tma.osd.mil)).

## Prison Time for a COR

On October 11, 2006, Bonnie Murphy, a former DoD employee, was indicted on charges for accepting an illegal gratuity and for accepting compensation to her federal salary. Murphy, a civilian disposal officer working in Iraq, allegedly accepted jewelry from a contracting firm, referred to as Company A, in exchange for helping

them secure and maintain three U.S. Army service contracts.

While in Iraq, Murphy was a member of the Defense Reutilization and Marketing Service team. She was responsible for identifying the needs of and requesting service contracts for the collection, removal, storage, and disposal of materials

from U.S. Army facilities. Murphy also had the authority to recommend specific contractors and to act as the contracting officer's representative (COR) for service contracts.

Beginning in July through December 2004, Murphy received

*Continued on page 3*

## Prison Time for a COR Cont'd

approximately \$9,000 worth of jewelry from employees at Company A. In return, Murphy helped Company A secure three U.S. Army service contracts: one for the disposal of hazardous materials, one for the removal of contaminated soil, and another for the removal and storage of used lithium batteries.



Before each of these contracts were awarded, Murphy wrote statements of

work requesting that the Army hire outside contractors for these services. She recommended to her supervisors that Company A be hired. Murphy also wrote a sole source justification letter recommending that Company A receive one of the contracts without undergoing a competitive bidding process.

On November 6, 2006, Murphy pled guilty to one misdemeanor count of conflict of interest in exchange for

prosecutors dropping the felony bribery charges. She is currently awaiting sentencing and faces up to one year in prison.

The maximum penalty for accepting an illegal gratuity is two years in prison plus a \$250,000 fine. The maximum penalty for accepting supplementation to a federal salary is five years in prison plus a \$250,000 fine.

## Assessable Unit Managers' Corner

One of the many responsibilities of the Assessable Unit (AU) Manager is to ensure that internal control reviews and testing are conducted properly and in a timely manner.

On October 23, 2006, the MIC Program Office forwarded the tasker for the FY 2007 Self Assessment Reviews, which are due February 28<sup>th</sup>.

This Self Assessment Review is designed to assess the organization's internal controls and determine if they are effective, efficient, and operating as intended. The review will identify internal control weaknesses requiring corrective action and/or provide each manager with the opportunity for implementing new internal controls or initiating improvements to existing



controls. A minimum of **three people per AU** must participate in the Self Assessment Review. The review should reflect a consensus of all the participants.

## Audit Reviews Highlight Internal Control

Despite DoD's efforts to improve contract management, changes in the acquisition environment related to increased reliance on contractors and new alternative contracting methods have caused DoD Contract Management to remain on GAO's high risk list. As required by the National Defense Authorization Act for Fiscal Year 2006, the GAO reviewed the vulnerabilities that the DoD faces with regard to contracting fraud, waste, and abuse as well as the actions DoD has taken to address these vulnerabilities. GAO found five key areas of weaknesses: sustained senior leadership; capable acquisition workforce; adequate pricing; appropriate contracting approaches and techniques; and sufficient contract management. **If the DoD does not implement effective internal controls, their contract funding will remain vulnerable to fraud, waste, and abuse.** To read more about this report (GAO-06-838R) please visit [http://www.ha.osd.mil/mhscio/Man\\_Ctrl\\_Prog\\_Audits.htm](http://www.ha.osd.mil/mhscio/Man_Ctrl_Prog_Audits.htm).

In their November 16, 2006, report on Defense Business Transformation, the GAO reported that although DoD has made some progress in establishing the procedures and management structures needed to successfully transform its business operations and address its high risk areas, significant challenges remain. Two of the major recommendations included: establishing a comprehensive, integrated, and enterprise-wide plan to guide its overall business transformation efforts and appoint a chief management official with the authority, experience, and tenure needed to successfully oversee these efforts. The GAO also stated in the report that **"establishing effective system modernization management controls... can increase the chances of delivering cost-effective business capabilities on time and within budget."** To read more about this report (GAO-07-229T) please visit [http://www.ha.osd.mil/mhscio/Man\\_Ctrl\\_Prog\\_Audits.htm](http://www.ha.osd.mil/mhscio/Man_Ctrl_Prog_Audits.htm).



*"At a time when DoD is competing for resources in an increasingly fiscally constrained environment, it is critically important that DoD get the most from every defense dollar."*

# What Do PRESENTS and the MIC Program Have in Common?



They are both something you enjoy all year!



## THE MIC PROGRAM HELPS ENSURE:

**P**rotection



Programs and resources are protected from fraud, waste, mismanagement, and misappropriation of funds.

**R**isk Assessment

Risks are assessed annually to determine the susceptibility of an activity to fraud, waste, and mismanagement.

**E**fficiency



Internal controls are effective and efficient in preventing fraud, waste, and mismanagement.

**S**elf Assessment Reviews

Periodic reviews are conducted to determine if necessary controls are in place and producing the intended results.

**E**ssential

Everyone is responsible for the essential internal controls that are necessary for the successful achievement of the organization's mission.

**N**umbers



Financial reporting is reliable.

**T**esting

Internal controls are tested and weaknesses are addressed.

**S**tandards



The 5 GAO's Standards for Internal Control (Control Environment, Risk Assessment, Control Activities, Information and Communications, and Monitoring) are appropriately considered.

