



Chief Information Officer Managers' Internal Control Program



INFORMATION BULLETIN

Volume 5, Issue 1

January 1, 2008

Special Note:

The annual CIO MIC Program Training is now available on MHS Learn. All CIO staff (Military, Government, and appropriate contractor personnel) are required to complete annual training no later than January 31, 2008.

"Information is one of our organization's most valuable resources and as such, requires responsible management by all personnel."



DoD's New Chief Management Officer

Deputy Secretary of Defense Gordon England has been officially designated as DoD's first Chief Management Officer (CMO). The position/designation is identified in the newly signed Deputy Secretary of Defense Directive (DoDD 5105.02).

The DoD CMO shall:

- Ensure Department-wide capability to carry out the DoD strategic plan in support of national security objectives.
- Ensure DoD's core business missions are optimally aligned to



support its warfighting mission.

- Establish performance goals and measures for improving and evaluating DoD's overall economy, efficiency, and effectiveness; and monitor and measure the department's progress.
- Develop and maintain a Department-wide strategic plan for business reform.

This is a welcome change for many lawmakers.

Senator Daniel Akaka (D-

Hawaii) stated that "Management challenges have plagued the department for years, and the establishment of a chief management officer is a necessary step to address them." **Senator John Ensign (R-Nevada)** stated that "I'm hopeful this will help bring more efficiency and oversight to the day-to-day business operations..."

For a copy of DoDD 5105.02, visit the document library on the MHS CIO website at http://www.ha.osd.mil/mhscio/doc_library.htm.

Managing Personnel Access

In an effort to help maintain the security of our information and information systems, managers must ensure that access privileges, held by their personnel, are appropriately monitored. Access privileges should be addressed not only for personnel departing the office, but also for personnel transitioning due to the current reorganization.

Directors/Managers should be vigilant with regard to changes to re-

quired access. They should regularly assess access to the following items/areas:

- secure websites;
- office files;
- files located on shared drives;
- information systems;
- databases;
- secure office locations, such as those requiring access cards; and



- Outlook mailboxes, calendars, and files.

Tips to Consider:

1. Access to information should be granted based upon the individuals' need for access to perform their duties.
2. Periodic reviews should be conducted to ensure that user access privileges are current and the privileges granted are appropriate/authorized.

DoD's Check-It Campaign Still Going Strong

Deputy Secretary of Defense Gordon England and DoD Comptroller Tina Jonas were two of the many honored guests at this year's DoD Managers' Internal Control Program and Check-It Campaign Conference held on November 28 and 29, 2007. Secretary England and Ms. Jonas spoke to attendees about the importance of internal controls and the success of DoD's Check-It Campaign.

When delivering his speech, Secretary England sported a red Santa hat to remind DoD managers "to check their lists twice to enforce internal controls within the department."



Internal controls are critical as the DoD manages a budget

of \$500 billion plus, not including costs associated with the war, England told attendees. He also stressed that the way internal controls are enforced within the department has a direct impact on our Military men and women currently serving on the front lines. He said that "they count on us every single day. They count on us doing this job, and they count on us doing it right. And we know that we do it right when we check it every day."

Secretary England referred to DoD's Check-It Campaign as the key to this goal. The purpose of the campaign, which began in July 2006, is to remind all DoD employees of the importance of their jobs to the overall mission and the importance of check-

ing their work to make sure it gets done right.

Ms. Jonas told DoD managers that they are the ones making it happen. The program is paying off through greater returns on investments and in savings of hundreds of millions of dollars. Ms. Jonas also noted that there has been an 84% reduction in the amount of self-identified internal control weaknesses since 2001 and that by 2006 the department had six entities with clean audit opinions.

Like the campaign's slogan says, **Check It. What gets Checked, Gets Done!**

Source: American Forces Press Service

The Softer Side of Internal Controls

So what are "soft" internal controls? Soft internal controls focus on the human aspect of internal controls. Examples include integrity, ethical values, trust, competency, management's philosophy, and commitment. Soft internal controls are essential components of any organization. They are intangible and difficult to verify, nevertheless, vital to the success of an organization.

Integrity and ethical behavior are the products of the 'organizational cul-

ture' (i.e., ethical and behavioral standards, how they are communicated, and how they are practiced). Management must exhibit strong core values, such as integrity and trust. This sends a message to all employees that they are expected to be ethical and trustworthy. **Management's actions establish the "tone at the top."**

Soft internal controls help establish the foundation for other traditional internal controls, such as policies and procedures. Managers must empha-

size the importance and commitment of ethics and integrity in everyday decision making, at all levels, to ensure organizational success.

Code of Ethics

1. Public service is a public trust, requiring employees to place loyalty to the Constitution, the laws and ethical principles above private gain.
2. Employees shall not...

Basic Email Etiquette to Remember

1. E-mail is not private.
2. Treat it as an official record.
3. Be concise.
4. Do your complaining elsewhere.
5. Don't speculate about things you do not know.
6. Email messages reflect upon you and the organization.
7. Spelling, grammar, and punctuation do count.
8. Be careful with subtlety, sarcasm, and humor.
9. Keep personal messages to a minimum.
10. Your tone can be heard in an email.
11. Read it two or three times before you send it.
12. Think before you send.



Remember, your email projects a perception of you and the organization. Think twice before you press send.

Internal Control Breakdown Costs DC Tax Office Millions

Two former DC Office of Tax and Revenue employees, Harriett Walters and Diane Gustus, were arrested and charged with numerous felony offenses for allegedly orchestrating a multi-million dollar property tax refund scheme. Walters, a mid-level manager in charge of property tax refunds, and Gustus, a tax specialist, used their positions to prepare and approve false property tax refunds. The refunds were used to prepare over 40 fraudulent checks averaging over \$388,000 each.



The checks were made out to phony corporate accounts controlled by Walters's relatives. With the help of a former Bank of America employee, the refund checks were cashed and distributed to co-conspirators, other friends, and family members.

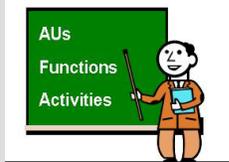
Officials have traced over \$20 million in fraudulent refund checks going as far back as the year 2000. That number is expected to increase as the investigation into Walters, Gustus, and other suspected tax and revenue employees continues.

Raids on the suspects' and their families' homes turned up thousands of dollars worth of designer clothes, shoes, and handbags, expensive jewelry, and several luxury vehicles.

To date, 10 people have been arrested in connection with the largest theft ever uncovered in local government in the DC area.

Assessable Unit Managers' Corner

Assessable Unit (AU) Managers, whose office mission has changed as a result of the current reorganization, will need to reassess their AUs to include the functions and activities. AU definitions may be updated to reflect minor changes, or if major changes have occurred, the AU itself



may need to be changed.

When proposing new AUs, AU Managers should submit the name and definition of the AU, as well as, a list of all applicable functions and activities. Once the AU has been accepted by the MIC Program Office, AU Managers should ensure that risk assess-

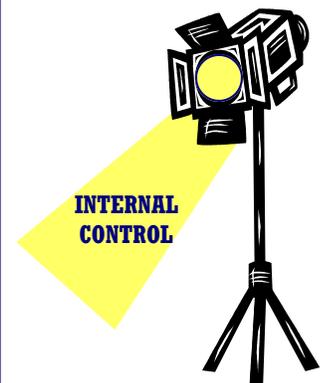
ments are conducted for each activity associated with the new AU.

We are aware that many of the changes associated with the reorganization will take time. However, we strongly encourage offices to begin assessing their AUs as they assess their new mission areas.

Audit Reviews Highlight Internal Control

DoD IG has released a summary report of the information assurance (IA) weaknesses identified in 36 audit reports from the GAO, DoD IG, and Army, Navy, and Air Force audit agencies between August 2006 and July 2007. The results identified a wide range of weaknesses. The most common were found in the following IA areas: access controls; Privacy Act information; security awareness, training, and education; and security policies and procedures. These are persistent problem areas for DoD. Many of the IA weaknesses identified in this report were also included in eight other IG summary reports. If unaddressed, these weaknesses will impact DoD's ability to mitigate or prevent the risks associated with operating in a shared IT environment. To read more about this report (D-2007-123), please visit http://www.ha.osd.mil/mhscio/Man_Ctrl_Prog_Audits.htm.

During their review of Defense Business Transformation, GAO found that although the DoD has made progress toward establishing a framework for overall business transformation they still must overcome two critical challenges in order to maintain and further the progress. The first challenge concerns DoD's lack of a comprehensive, integrated, and enterprisewide plan or set of linked plans supported by a planning process that sets a strategic direction for overall business transformation. The second is that DoD has not established a full time leadership position dedicated solely to the planning, integration, and execution of business transformation efforts (DoD recently designated the Chief Management Officer). Until DoD addresses these issues, they will be challenged to integrate related initiatives into a sustainable, enterprisewide approach to resolve weaknesses in business operations that are at high risk of fraud, waste, and abuse. To read more about this report (GAO 07-1072), please visit http://www.ha.osd.mil/mhscio/Man_Ctrl_Prog_Audits.htm.



"Far more powerful than what is stated or preached are the actions demonstrated and reinforced by those at the top."