



**Information Management, Technology & Reengineering  
and Joint Medical Information Systems  
Managers' Internal Control Program**



**INFORMATION BULLETIN**

Volume 4, Issue 2

March 30, 2007

**Spring is Here!**

- S** – Security
- P** – Processes
- R** – Reviews
- I** – Internal controls
- N** – Necessary
- G** – Greater results

**No matter the season, internal controls are important.**



*“Internal controls ensure that what should happen, does happen EVERY DAY- but they must be in place, effective, and used.”*

**DoD’s “Check It” Campaign Promotes Internal Control Awareness**

DoD has kicked off a year long campaign aimed at raising awareness on the importance of effective internal controls. The campaign’s title is “Check It, What Gets Checked, Gets Done.” “This is a big title, but a simple concept that will have very, very powerful results here in the department,” said Deputy Secretary of Defense, Gordon England.

The goal of the “Check It” campaign is to reach everyone throughout DoD. It will remind them of the importance of their jobs to the overall mission and the importance of checking what they do



ensure it gets done right. “Checking it pertains to just about anything that depends on a process,” said Peggy Johnson, Program Manager for DoD’s Managers’ Internal Control Program.

The DoD internal control campaign is spreading a simple message - **Every job, no matter its size, is important.** We want to do the work right the first time. So we want everyone to **“Check It,” because what gets checked gets done right.**

To make sure the message gets to as many of the 2.6 million civilian and military

employees as possible, DoD has developed public service announcements for many of its major functional areas.

To view the “Check It” campaign public service announcements for the Acquisition, Information Technology-Net Centric, and Financial areas, please visit the Managers’ Internal Control Program page located on the MHS CIO Website at [http://www.ha.osd.mil/mhscio/Man\\_Ctrl\\_Prog.htm](http://www.ha.osd.mil/mhscio/Man_Ctrl_Prog.htm).



**Annual Reporting on Internal Controls**

The DoD Managers’ Internal Control (MIC) Program consists of two distinct processes which require annual reporting: 1) the *Federal Managers’ Financial Integrity Act (FMFIA) Overall Process*; and 2) the *FMFIA Over Financial Reporting Process*.

The *FMFIA Overall Process* pertains to the overall program, operational, and

administrative controls, whereas the *FMFIA Over Financial Reporting Process* pertains to the processes, procedures, and systems used to prepare, compile, and generate the DoD financial statements.

Every year the head of each executive agency is required to submit a report to Congress on whether there is reasonable assur-

ance that the agency's controls are achieving their intended objectives.

The Director, IMT&R submits an Annual Statement of Assurance (ASA) report which covers the FMFIA Overall Process. This ASA addresses the evaluation of the IMT&R/JMIS MIC Program. It represents the

*Continued on page 2*

## Annual Reporting on Internal Controls Cont'd

Director, IMT&R's informed judgment as to the overall adequacy and effectiveness of internal control within the organization.

The ASA report includes: *TAB A* - an evaluation of the organization's MIC Program; and, if required, *TAB B* - documentation on a reportable condi-

tion that is significant enough to report to the next higher level of management.

The Self Assessment Reviews performed by each office also contribute to the ASA. They provide the Director, IMT&R with reasonable assurance

that internal controls are working effectively and efficiently, and **that management, at all levels, is involved in the process.**



Once the ASA is approved, it is submitted to the TMA MIC Program Office for inclusion in the TMA ASA.

## Policies – Consequences and Enforcement

One of the lessons learned from last years slew of data security breaches is that there is no real value in implementing policies, if you do not ensure that they are enforced. Policies often address what employees must do and what they should not do, but what many do not address are the consequences of violating these policies.



**clearly define the consequences of non-compliance.**

Management must be actively involved in the policy process from approval to enforcement. What management considers important, employees will also consider important.

Management must ensure that all personnel, at all levels, are aware of the organization's policies and that they understand the importance of complying with these policies.

It is essential for policies to address the penalties or disciplinary actions associated with non-compliance. Employees will be more likely to comply with the policies, if they are aware of the consequences for violating them.

Policies allow organizations to establish procedures and controls that will reduce risk. However, their effectiveness is directly proportional to the support they receive from everyone in the organization.

Effective policies should: **have support from the top down, be acknowledged by all employees, and**

## Internal Controls for Everyday Tasks

Everyone encounters internal controls in their daily business activities as well as in their personal lives, yet it is a subject that is often misunderstood, ignored, or undervalued. **Internal controls are the policies, procedures, guidance, and instructions that help mitigate or prevent risks.** They help to ensure that programs and resources are protected from fraud, waste, mismanagement, and misappropriation of funds. They help us ensure that mission and program objectives are efficiently and effectively accomplished. So, how can a subject of such importance be so unappreciated?

Perhaps, if we identify how internal controls are associated with the tasks that all of us perform everyday, we can better understand how internal controls can help us mitigate the risks associated with achieving our organizational goals.

The following provides examples of the risks associated with everyday tasks and the internal controls that help mitigate these risks.

### CAC Cards

**Risks:** Loss or theft; expired cards

#### **Internal Controls:**

- Display CAC Card Awareness Posters
- Store CAC Cards in a safe location when not in the office
- Check expiration dates routinely

### Securing the Office

**Risks:** Theft of office equipment or files; Theft or misuse of sensitive data

#### **Internal Controls:**

- Maintain daily security checklist
- Secure sensitive data when not in use

- Control access with security system

### Computer Usage

**Risks:** Misuse or loss of data; theft or damage of computer equipment; viruses



#### **Internal Controls:**

- Provide training on use of equipment
- Change passwords frequently
- Store computer equipment in a secure area
- Report any suspicious emails or files to Network Support immediately

**Recognizing the value of daily, routine internal controls is vital to the mission.**

## Jail Time for a Former Treasury Department Employee

David C. Faison, a former Treasury Department employee, was sentenced on February 26, 2007, to nine months in federal prison for stealing more than \$67,000 in uncut partially printed \$100 bills. Faison worked as a stock control recorder and was responsible for distributing currency paper within the Bureau of Engraving and Printing, which gave him access to the area where bills were printed.

From May 2006 through August 2006,

Faison stole 21 sheets of \$100 bills that were missing serial numbers and Treasury Seals. Authorities caught up with Faison after he tried to launder over \$37,000 through casino slot machines in New Jersey, West Virginia, and Delaware. Surveillance footage showed him feeding the counterfeit bills into slot machines, playing for a while, and then cashing out for new bills.

Faison was ordered to pay the federal government back the \$37,200 he fed

into slot machines. The remaining money was recovered from Faison's Maryland home hidden inside rolls of wrapping paper.

U.S. District Judge Paul L. Friedman sentenced Faison to nine months in federal prison and supervised release for three years after serving his prison time. Authorities say that Faison worked for the Bureau of Engraving and Printing for over 30 years.

## Assessable Unit Managers' Corner

**T**esting is not only an important part of the Self Assessment Review (SAR) process, but it is an equally important part of the corrective action process.

Assessable Unit (AU) Managers are responsible for ensuring that internal controls are **tested** during the SAR process to determine if they are

working effectively and efficiently.



They are also responsible for monitoring the development, implementation, and **testing** of corrective actions to ensure that internal controls are working as intended and that weaknesses truly are corrected.

The most commonly used **testing methods** are: *1) Confirmation/Verification; 2) Document Analysis; 3) Interview; 4) Questionnaire; 5) Sampling; 6) Observation; 7) Transaction Testing; and 8) Physical Examination.*

## Audit Reviews Highlight Internal Control

During their testimony before the Subcommittee on Oversight and Investigations of the Committee on Veterans' Affairs, the GAO stated that although the VA has taken some action to address their weaknesses, they still have not implemented the key elements of a comprehensive information security program. From 1998-2005 the GAO has issued 15 reports and testimonies addressing the ongoing weaknesses of the VA's information security program. Some of these weaknesses include lack of controls for areas related to: electronic and physical access to sensitive information; segregation of duties; software updates/changes; and continuity of computerized systems and operations. GAO attributed these weaknesses to the VA's lack of: defined roles and responsibilities; routine risk assessments; security policies and procedures; security monitoring; and ... "a process to measure, test, and report on the continued effectiveness of computer system, network, and process controls." To read more about the GAO's Testimony (GAO-07-532T) please visit [http://www.ha.osd.mil/mhscio/Man\\_Ctrl\\_Prog\\_Audits.htm](http://www.ha.osd.mil/mhscio/Man_Ctrl_Prog_Audits.htm).

According to the GAO's recent testimony on Federal Financial Management, DoD needs to transform its financial management and business practices that have a negative impact of both DoD's and the federal government's ability to: control costs; ensure basic accountability; anticipate future cost and claims on the budget; measure performance; maintain funds control; prevent fraud, waste, and abuse; and address management problems. DoD has made some progress in correcting these issues such as getting top level management officials engaged and developing the Financial Improvement and Audit Readiness plan, but more needs to be done to correct these long-standing weaknesses. GAO suggests that DoD (1) develop and implement a viable strategic plan with goals, objectives, key milestones, and measures to monitor and report on progress in transforming key business operations and (2) appoint a chief management officer to oversee its overall business transformation efforts. To read more about the GAO's Testimony (GAO-07-542T) please visit [http://www.ha.osd.mil/mhscio/Man\\_Ctrl\\_Prog\\_Audits.htm](http://www.ha.osd.mil/mhscio/Man_Ctrl_Prog_Audits.htm).



*"Agencies need to tackle long-standing internal control weaknesses by fully embracing the assessment, reporting, and corrective action approach called for in OMB's revised Circular No. A-123."*