



Information Management, Technology & Reengineering and Joint Medical Information Systems

Managers' Internal Control Program



INFORMATION BULLETIN

Volume 3, Issue 3

June 30, 2006

Special Point of Interest:

The Fiscal Year 2006 IMT&R/JMIS Annual Statement of Assurance was submitted on June 9, 2006. A special thanks to all AU Managers, MIC Program Representatives, and everyone else who helped put together this report.



"We serve in positions of trust and we must earn and maintain that trust through our actions on a daily basis."



Theft of Veterans Affairs Laptop Serves as a **WAKE-UP CALL** to All Agencies

The Government Accountability Office (GAO) and DoD Inspector General have been reporting for years that government agencies do not have adequate controls over access to social security numbers and other sensitive information. In fact, the GAO has identified information security as a government-wide high-risk issue since 1997. Today, nearly 9 years later, it appears that many government agencies still do not have the proper controls in place to protect this vital information.

The recent theft of a Veterans Affairs (VA) employee's laptop, containing personal information on 26.5 million veterans and 2.2 million service members, should serve as a prime example of just how important proper information security controls are. "When we think of cybersecurity, we focus on protecting vital information systems against intrusion by criminals and terrorists. We now see that all the high-tech fixes in the world cannot protect these systems against one employee who

disregards an established policy and one agency that does not take sufficient measures to ensure compliance with the policy," said Senator Susan Collins at a May 25 hearing on the VA incident.

In the weeks since the incident, the VA "has begun a relentless examination of its policies and procedures to make sure nothing like this happens ever again," said VA Secretary Jim Nicholson.

TMA Strengthens Information Security

Over the past three years TMA has made significant progress in promoting information security awareness in an effort to protect personally identifiable data.

In 2003, the TMA Privacy Office initiated Health Insurance Portability and Accountability Act (HIPAA) Privacy Training. This training provides an introduction to HIPAA and describes the appropriate uses and disclosures of protected health information (PHI). In 2005, the Privacy Office expanded the training to include HIPAA Security and annual HIPAA re-

resher courses. The purpose of the security training is to describe the proper safeguards for protecting PHI.

During the past few months TMA has continued its efforts in strengthening information security controls and increasing awareness over the importance of safeguarding sensitive or personally identifiable data. In response to the recent OMB memorandum titled, *Safeguarding Personally Identifiable Information*, the TMA Privacy Office, in cooperation with the MHS CIO, launched a policy review

and awareness campaign to ensure all TMA employees are aware of their responsibilities to protect and secure data.

As part of this initiative, the TMA Privacy Office required all TMA employees to complete security and privacy awareness training. The purpose of the training was to ensure all employees are aware of the policies related to safeguarding personally identifiable data, the penalties for the misuse of data, and the proper procedures for accessing and handling this data.

Continued on page 2

TMA Strengthens Information Security Cont'd

The TMA Admin Office recently distributed a copy of the TMA Security Program Standard Operating Procedure and TMA Security Program Guide to all employees. The purpose of this guidance is to ensure that all employees are aware of the security

procedures required of them.

The controls in these documents will help mitigate the security risks we all face on a daily basis. They will help us protect not only our own personal information, but they will help us pro-

tect the personal information of our fellow employees, service members, and veterans. For additional information please visit the Privacy Office's webpage at <http://www.tricare.osd.mil/tmaprivacy/default.cfm>.

Purchase Cardholders **BEWARE:** Misuse is Serious Business

Most people are aware that intentional misuse of the government purchase card constitutes fraud and is subject to disciplinary action and/or criminal penalties. However, what many people don't know is that even accidental use can carry similar punishments.

A Veterans Affairs (VA) employee was suspended for accidentally using his government charge card to purchase new tires for his car. The employee claimed that he had made an honest mistake. He stated that when he paid for the tires he must have

pulled the wrong card from his wallet. He also stated that he did not realize his mistake until the purchase card statement arrived later that month. The employee received a 30-day suspension despite returning the \$226 he had accidentally charged.



The 30-day suspension, which was originally dropped after the employee appealed his case, was reinstated by the VA's Merit Systems Protection Board. The Board stated that "misuse

of a government charge card is a serious offense," and that the intent was irrelevant. They felt the suspension was an adequate punishment.

Additional information on purchase card misuse can be found in the DoD General Counsel's new purchase card training, titled *Ethics Rules Regarding Misuse of the Government Purchase Card or Travel Card*. The briefing is available on the General Counsel's website at http://www.defenselink.mil/dodgc/defense_ethics/.

Are You Prepared?



In light of the recent emergency situation at Skyline, would you say your office was prepared? Emergency situations can happen at any time and in any place. They often catch us off guard, but there are things we can do to prepare in advance.

First and foremost, obtain a copy of the organization's emergency preparedness procedures and incorporate the specific needs of your office. These procedures should outline the plans your office has in place for various types of emergency situations. They should also outline the responsibilities managers and employees have in dealing with these types of situations.

In addition to reviewing emergency procedures, here are some questions you might ask yourself to ensure you are **always** prepared for an emergency.

"The best time to know what to do in an emergency is before, not after, it happens."

1. Do you know exactly what your office's procedures are for emergency situations and have you read them? (It is also a good idea to re-read these policies periodically.)
2. Do you know where your office's emergency procedures are located and do you keep a copy of them at your desk and at home?
3. Do you or does your office routinely review these procedures to make sure they are accurate and up-to-date?
4. Are all office personnel, especially new personnel, aware of these procedures?
5. Do you have a list of important phone numbers in your purse or wallet, or programmed into your cell phone?
6. Do you know where exit routes, stairways, fire extinguishers, and medical kits are located?
7. Do you have a supply kit containing a flash light, extra medicine (if needed), food, water, and comfortable walking shoes; and is it stored in your desk?

It is also important to note that during these types of situations you may not have access to your office or to your office's computer system. Offices should take this into account when developing emergency procedures.

Remember, it is everyone's responsibility to prepare themselves for emergency situations, but having the proper procedures in place can help by reducing risk and minimizing adverse effects.

Recent Investigation & Sentencing of Government Employee

On June 19, 2006, Allison Broda, a former government contract employee, was sentenced to one year in prison and ordered to help repay the government \$84,000 for accepting illegal gratuities.

Broda, who was a supply technician for the Space & Naval Warfare Systems Center Charleston (SPAWAR), had the authority to award freight transportation contracts on behalf of the U.S. Government. From March 2001



through November 2004, Broda accepted over \$10,000 in various gifts from Teresa Stranigan, a sales representative for Air Cargo in exchange for repeated contract awards. Some of these gifts included lunches, concert tickets, hotel accommodations, spa getaways, clothes, and jewelry. From 2001 to 2005, Air Cargo received a total of \$717,000 in freight contracts from Broda.

Broda wasn't the only one charged in this case. Stranigan received five months of house arrest and five years of probation and was ordered to help Broda repay the \$84,000 in excess charges the government claims they were overbilled from Air Cargo.

When asked why Broda received the stiffer punishment, the judge said it was because Broda was a government official and she was in a position of public trust.

Assessable Unit Managers' Corner

With the successful completion of this year's Annual Statement of Assurance, it's time to begin preparing for Fiscal Year (FY) 2007.

During the next few months, all Assessable Unit (AU) Managers should assess and document their current mission areas. This includes ensuring that all mission areas are covered by an appropri-

ate AU and ensuring that all AUs are documented by current functions and activities.

Beginning FY 2007, the MIC Program Office will establish an internal control Senior Management Council. The council will be chaired by the MIC Program Manager and comprised of all IMT&R and JMIS AU Managers. The pur-

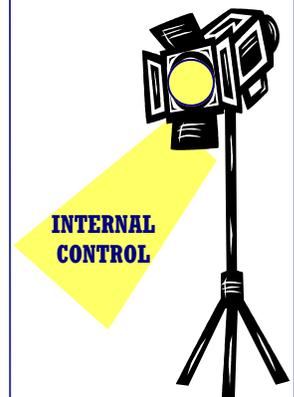
pose of the council is to provide an opportunity for managers to discuss any IMT&R and JMIS organizational issues concerning internal controls.



Audit Reviews Highlight Internal Control

In response to the recent information security breach, Congress requested that the GAO conduct a review of the VA's Information Security Program; examine ways agencies can prevent misuse of personal information; and examine the procedures for proper notification of security breaches. In their findings, the GAO stated that the VA continues to have weaknesses over access controls, physical security, and proper segregation of duties. They found that while some progress has been made, the VA still has not developed a sufficient information security program. In order to address these much needed changes, the VA will need "strong leadership, sustained management commitment and effort, **disciplined processes**, and consistent oversight." To learn more about the GAO's findings please visit <http://www.gao.gov/new.items/>

The scope of the recent DoD IG Audit on the acquisition of AHLTA was to review program requirements, Clinger-Cohen Compliance, and management controls. During their review, the IG found that AHLTA's program management office is utilizing "risk management, lessons learned, and performance monitoring to mitigate cost, schedule, and performance risks." **They also determined that AHLTA's management controls were effective and stated that no weaknesses existed in the management control documentation they reviewed.** The review did, however, identify weaknesses in other areas. The IG reported that the mitigation techniques the program management office had in place were not sufficient enough to adequately reduce and control risk, especially the risk involved in using commercial off-the-shelf products. To read more about the IG's findings and the Program Offices response please visit <http://www.dodig.osd.mil/Audit/reports/FY06/06-089.pdf>.



"Internal controls are an integral part of an organization's processes and are not a superimposed set of requirements."