



Chief Information Officer Managers' Internal Control Program



INFORMATION BULLETIN

Volume 7, Issue 3

June 30, 2010

Special Message:

Alice Campbell retired this April after building a robust and dynamic Managers' Internal Control Program for OCIO.

Thank you, Alice!

May you look to the past with pride and to the future with anticipation and pleasure!



"A wise man learns by the experience of others."

Risk Management Taps New Resource

The Office of the Chief Information Officer (OCIO) recently began establishing formal communities of practice through the Performance Improvement Division. As an inaugural effort, the Risk Management Community of Practice, (RM CoP) launched on June 10, 2010. With the support of Michael Landry, OCIO Risk Management Subject Matter Expert (SME), and the assistance of the CIO Managers' Internal Control Program (MICP), a group of risk management (RM) practitioners from across OCIO gathered to share ideas and confide in one another regarding RM practices. Acknowledging the need for discussion and access to new knowledge in the risk field, members recognized the benefit of an RM CoP for managing change related to risk.

The main goal of the RM CoP is to institutionalize excellence in RM by standardizing the level of RM effort throughout the organization, improving the level of risk management and ultimately improving performance. To achieve this goal, appropriate RM practices must become embedded in normal day-to-day operations to the point of being

second nature. The embedding of RM practices is both the result and a major benefit of a successful RM CoP. "Best practices for managing risk are in essence internal controls, and as such should become part of the fabric of everyday business, never "extra" work," stated Annette Sorah, Coordinator for the CIO MICP.

According to SME Michael Landry, "Risk transcends all of our individual areas of focus. It takes a community to be successful, which the Risk Management Community of Practice provides." Members bring individual perspectives, a variety of skill sets, and different practical experiences to the community. This creates a domain knowledge which, in conjunction with the social network aspect of the community, becomes a valuable resource for all. By creating a medium for effective risk management, the RM CoP will provide the opportunity for diverse courses of action, while promoting the desired enterprise level of practice.

At the first meeting, members learned CoPs provide a level playing field, overcoming

barriers to communication frequently posed by organizational boundaries. Overcoming these barriers facilitates innovation through disseminating valuable information, establishing processes, improving productivity and allowing formation of consensus within the community.

Whether as individuals or as a group, RM practitioners face the challenge of taking full responsibility and owning their risk. When done correctly, fear, lack of trust, and admission of risk management failure cease to be issues. Taking ownership enables members to carry knowledge and best practices from the RM CoP back to their individual offices to share with their teams. Communication is key. Risk managers must communicate to their teams the best practices they have brought out of the RM CoP. In return, teams must communicate new risks and mitigation strategies to their managers to take back to the community.



Security & Safety Require Vigilance

Many of us work behind locked doors. At the very least, in most offices one person performs the duties of receptionist in addition to other work. We all wear identification badges, and maintenance workers wear uniforms. We use CACs to access our computers. We are accustomed to the occasional visitor or repair person who does not wear ID or a uniform. Under these circumstances we easily become complacent about security and safety. We can become so comfortable in our surroundings that we stop really looking at those badges or uniforms. We may not be vigilant about enforcing security procedures. When we behave this way, we make fooling us easy.

Recently, an unauthorized person gained access in skyline to non-public space under the pretense of

checking the sprinkler system for leaks. Although he had no identification, or even a toolkit, and borrowed a chair to reach the ceiling, no one became suspicious. The thief stole \$200 from a wallet left in a coat pocket.

It could have been worse. A little extra caution, a little more vigilance might have prevented the incident.

Tips for Security & Safety

- 1. Stay aware.** Do not get so caught up in work, conversation, or just your own thoughts that you cease to be aware of people and events around you.
- 2. Keep your ID displayed in plain view.** Don't tuck it away in your pocket or otherwise obscure it.



Doing so defeats the purpose of wearing identification in the first place.

- 3. Verify the identity and purpose of visitors you do not recognize. Notice unusual behavior.** If you are uneasy get help. As part of standard security procedures for your area, you should know how and to whom to report suspicious activities or individuals. If you don't know, make it a point to find out.
- 4. Know and follow all the security procedures for your office, suite, and/or building.** This includes keeping your valuables secure. Leaving your iPhone, purse/wallet or other valuables unsecured begs a thief to steal them.

New Look for MHS CIO Website!



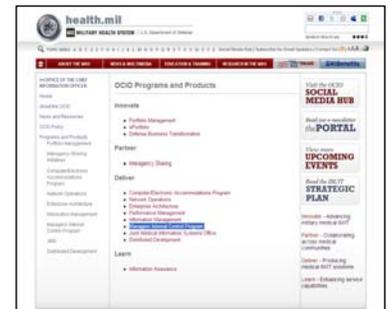
<http://www.health.mil/MHSCIO>

Same address, and all the great information, plus many new and exciting places to explore. The difference, a new look and navigation changes.

To access the Managers' Internal Control Program webpage:

- (1) Select Programs and Products** on the left.

- (2) Select Managers' Internal Control Program.**



- (3) Select a topic.** You can still find everything: Training, Guidance, References, back issues of the Information Bulletin.



Please visit the new MHS CIO Website.

Marine Captain Charged with Contract Skimming

Capt. Eric Schmidt, along with his wife, Janet Schmidt, was charged on March 4, 2010 with two felony counts of conspiracy to commit wire fraud and filing a false tax return that concealed illicit income from the Internal Revenue Service.

According to criminal information filed against them, Capt. Schmidt used his position in the contracting process to steer contracts to his favored Iraqi contractor, and falsely certified the type and

quantity of goods and their source as being the Iraqi contractor. Mrs. Schmidt found United States based vendors to provide the goods, often purchasing inferior products or fewer than specified in the contracts. She then arranged delivery of these goods to the Marines in Iraq.

Investigators have determined the Schmidts collected a total of approximately \$1.75 million in illegal payments during Capt. Schmidt's one-year

deployment to Iraq. They failed to report any of the illegal payments on their tax return, resulting in the tax evasion charges.



If found guilty, each defendant faces a statutory maximum of 23 years in federal prison.

To read more about this case, please visit: <http://www.justice.gov/usao/cac/pressroom/pr2010/042.html>

Assessable Unit Managers' Corner

Annual Statement of Assurance (ASA) signed May 19, 2010, ahead of schedule. Thank you for all your hard work and diligence providing input from your Divisions and Program Offices.



DoDI 5010.40 Re-issued.

February 17, 2010 the Department of Defense re-issued Instruction Number 5010.40, Managers' Internal Control Program (MICP) Procedures, documenting changes in MICP requirements. It includes a new requirement for Assessable Unit (AU) Administrators who are government employees.

The AU administrators will assist the AU managers, assuming some of the roles and responsibilities that previously belonged to MICP Representatives. MICP Representatives, who may be contract personnel, should continue performing their current roles unless informed otherwise by their AU Managers.

Audit Reviews Highlight Internal Control

As a result of a study on Defense Infrastructure, GAO reported April 30, 2010, that Army failed to establish a framework for monitoring achievement when it set goals to reduce construction costs and building timelines. Without activities in place to monitor performance measures and indicators needed to compare actual performance to planned or expected results, it is not clear that the Army's expanded use of wood materials and modular building methods will achieve the intended purpose of reduced facility costs over the long term. During the review, senior Army headquarters officials acknowledged that a framework to measure goal achievement should have been established when the cost and timeline goals were instituted. The officials also stated that the only explanation for not monitoring the goals was that they were so involved in implementing the many changes adopted under the Army's military construction transformation strategy that no one took the time to monitor and track the results being achieved from the changes. To read more about this report (GAO-10-436), please visit <http://www.gao.gov/new.items/d10436.pdf>.

Despite numerous recommendations provided by GAO over the past several years, one government agency has made only limited progress in resolving long-standing deficiencies in securing its information and systems, according to GAO testimony before a Subcommittee on Oversight and Investigations, U.S. House of Representatives, released May 19, 2010. Ongoing deficiencies in five major categories of information security controls: access control, configuration management, segregation of duties, contingency planning, and security management, continue to be a problem for the agency. Additionally, GAO reported that in the agency's fiscal year 2009 performance and accountability report, an independent auditor stated that IT security and control weaknesses remained pervasive, placing agency's program and financial data at risk and leaving the agency vulnerable to disruptions in critical operations, theft, fraud, and inappropriate disclosure of sensitive information. To read more about this report (GAO-10-727T), please visit <http://www.gao.gov/new.items/d10727t.pdf>.



“Identifying your starting point is the first step in defining your goal.”