



Chief Information Officer Managers' Internal Control Program INFORMATION BULLETIN



Volume 8, Issue 2

June 30, 2011

Special Message

The CIO Managers' Internal Control Program has a new Program Manager! Please welcome **Angela Prater, Deputy Director of Performance Improvement Division**. A member of the Performance Improvement Team since 2007, Angela joined the ranks of government in late March this year, bringing a fresh perspective to the CIO MICP



All things have risk. It is the consequences, and the consequences of consequences, that dictate the level of our response to the risk.

DoD Serious About Internal Controls

According to the Department of Defense (DoD) Managers' Internal Control Program (MICP) webpage¹, during Fiscal Year 2010 the Office of the Secretary of Defense (OSD) Comptroller, in accordance with DoD Instruction 5010.40, briefed the specific requirements/attributes of an effective MICP with each of the 36 Components that are currently required to submit the Annual Statement of Assurance to OSD. The briefings emphasized the following:

- Importance of Director Support (aka "Tone-at-the-Top");
- Reliance upon a "Risk-based Framework";
- Implementation of "Self-Reporting Concept";
- Leverage of the Component's in-house Expertise.

This spring Steve Silverstein, DoD MICP, was a speaker at the *DoD Business and Financial Improvement Leadership*

Conference, held March 23-24. Mr. Silverstein briefed² DoD's 2010 MICP accomplishments and the new strategic approach to internal controls, reinforcing the key areas of emphasis listed above. These same concepts are embodied in CIO MICP practices.



Importance of Director Support (aka "Tone-at-the-Top")

For better or worse, an organization's leadership sets the "Tone-at-the-Top" which influences the atmosphere of the workplace, all the way to the lowest levels of the organization. Unethical, fraudulent, and/or wasteful practices are less likely to occur in an environment where the journey is nearly as important as the destination. On the other hand, an environment in

which the end justifies the means frequently promotes disregard for ethical behavior, which can lead to fraud, waste and misuse of assets, and/or misuse of power. History provides numerous examples of these kinds of problems.

DoD considers the "Tone-at-the-Top" an essential ingredient of a successful internal control program, calling it "the most important component of the control environment,"¹ and emphasizing the need for senior management's support through communication, active participation, self-reporting, and recognition of successful internal control activities. All levels of management set the tone. When managers at every level understand and communicate the importance *and benefit* of good controls, that same understanding and acceptance is more likely to be sustained through to



Continued on page 2

DoD Serious About Internal Controls, continued

the execution level, and effective internal controls are more likely to be implemented on a continuous basis.

Reliance upon a "Risk-based Framework"

Identifying, documenting, and ranking risks is crucial to preventing risks from becoming reality and/or mitigating the results when risks do become reality, especially risks associated with mission aligned activities.

Risk	Likelihood	Impact	Mitigation
...
...
...

Pretending that risks don't exist is self-delusion, and a poor management practice. This kind of denial usually is caused by fear, and leads to the false assumption that having risk reflects poorly on an organization or its managers. The truth of the matter is that identifying potential risk is part of a good risk management program, and speaks to the quality of the risk identification processes in place in the organization. Everything has some degree of risk, and sometimes minor risks lead to major risks and possible serious impact on the organization and its goals. Admitting the fact that there is risk is the first step in managing the risk. Weaknesses stem from unmanaged or poorly managed risk. Identifying risk

provides the opportunity to develop good controls to manage the risk. Remember, a risk is a potential adverse event, not a certainty. An adverse event which is a certainty, regardless of preventative measures, is an issue. Once an issue occurs, mitigation/damage control is the only recourse.

Implementation of "Self-Reporting Concept"

Increased emphasis is placed on candid communication of identified risks and recommendations for remediation through the "chain of command."² The same applies to weaknesses. This is especially important regarding risks or weaknesses which might materially impact the organization. Leadership is encouraged to develop a business culture in which candid self-reporting is rewarded rather than punished. Fear is the factor that most often determines whether risks and weaknesses are reported. Individuals may be afraid of retribution or just embarrassment. Fear is counter-productive. The goal is to identify and remediate problems early from the inside, before they can escalate, rather than waiting for a Government Accountability Office or DoD Inspector General audit to uncover them. Risks evolve and so do weaknesses. Admitting that a risk or weakness

has developed is beneficial. It provides the opportunity to ensure the risk is addressed or the weakness corrected, and done so in a timely manner.

Leverage of the Component's in-house Expertise

Each Division/Program Office has employees who are experts in their functional areas. It only makes good sense to leverage that expertise in developing, reviewing, and assessing the effectiveness of procedures, processes, administrative controls, etc. Here again, candor is essential. If a risk or other problem is identified, employees must feel free to communicate the situation to appropriate authority without fear and be confident that the risk/problem will be addressed. Objectivity is also crucial. The importance of objectivity is why the CIO MICP requires a consensus of at least three individuals when conducting Self-Assessment Reviews of the internal controls for each Assessable Unit. Multiple viewpoints help ensure objective assessment of the value and effectiveness of the controls being reviewed.



¹<http://comptroller.defense.gov/micp.html>

²*Department of Defense Managers' Internal Control Program, Challenges, Accomplishments and Recognition, March 24, 2011, UNCLASSIFIED* (http://comptroller.defense.gov/micp_docs/training_and_events/FY2011_DoD_BFIL_Conference/Steve_Silverstein.ppt)

Small Thefts — Big Penalty

May 19, 2011 - As part of a guilty plea, a former Department of Defense civilian employee, Tyrone L. Ellis, admitted to approving Army Emergency Relief (AER) loans and grants to dozens of service members and their families in financial need in amounts greater than necessary, then requesting and receiving approximately \$9,250 back from the recipients and converting the returned funds to his own use. In

addition he admitted making false statements to investigators when questioned about the allegations.

AER is a private, non-profit organization that serves as the emergency financial assistance organization for the U.S. Army. AER's operations are financed by voluntary contributions from active and retired soldiers during

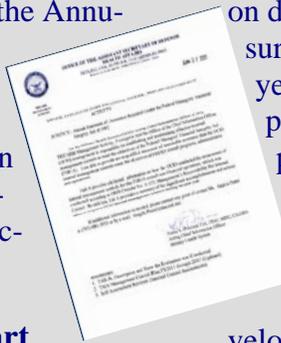
an annual fund raising campaign, as well as by unsolicited contributions, repayment of outstanding loans and income from reserve funds.

Sentencing is scheduled for August 2011. Ellis faces up to 10 years in prison and a fine of \$250,000. To read more, please visit: <http://www.justice.gov/opa/pr/2011/May/11-crm-641.html>



Assessable Unit Managers' Corner

“Thank You!” to everyone involved in producing the Annual Statement of Assurance – from accumulating and providing information to review and coordination of the final document.



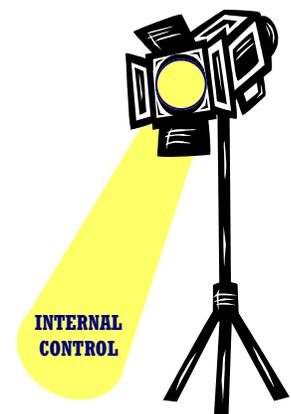
Now it's time to start documenting input for FY 2012.

DoD is placing renewed emphasis on developing “Statement of Assurance content throughout the year,”² and maintaining supporting documentation. So, please do not wait for a data call before beginning to identify items for inclusion in the Annual Statement of Assurance. Each office should develop an easy method of accumulating ASA data throughout the

year. It could be as simple as making a reminder list of events/topics to be expanded later, or as comprehensive as producing draft input periodically throughout the year. Last year's ASA data call questions are the perfect starting point for identifying, gathering, and documenting potential ASA inputs from events and awards, procedures, or other relevant data.

Audit Review Highlights Internal Controls

In a report released May 10, GAO stated that internal control weaknesses limit the Transportation Worker Identification Credential (TWIC) Program's ability to provide reasonable assurance that access to secure areas of Maritime Transportation Security Act regulated facilities is restricted to qualified individuals. When developing the program, the Transportation Security Administration did not assess internal controls designed or already in place to determine whether they provided reasonable assurance that they could meet defined mission needs for limiting access to appropriate individuals. In addition to these weaknesses in pre-credentialing processes, controls for ensuring that TWIC-holders maintain their eligibility were not identified, nor was a cost-benefit analysis conducted. Although DHS has not demonstrated that TWIC, as currently implemented and planned, is more effective than prior approaches used to limit access to ports and facilities, GAO states that conducting a regulatory analysis using information obtained from internal control and effectiveness assessments as the basis for evaluating costs, benefits, security risks, and corrective actions could help ensure the TWIC program is more effective and cost-efficient than existing measures or alternatives for enhancing maritime security going forward. To read more about this report (GAO-11-657), please visit <http://www.gao.gov/new.items/d11657.pdf>



Prevention is usually easier and more cost effective than mitigation.