



Chief Information Officer Managers' Internal Control Program



INFORMATION BULLETIN

Volume 6, Issue 3

June 30, 2009

Special Message:

The CIO's Annual Statement of Assurance was successfully submitted two days prior to the suspense date. A special thanks to all Assessable Unit Managers and MIC Program Representatives for all their hard work and support in putting together this report.



“Ethical behavior is the bedrock of mutual trust.”

Ethics Is Everyone's Responsibility

There are several dictionary definitions regarding ethic, ethics, and ethical behavior all of which relate to a “system of moral principles or values.” Without getting into a complex philosophical area, a simplistic definition of ethical behavior is “to do the right thing, because it is the right thing.” The “right thing” is determined by the values of the organization. Ethical behavior is the demonstration of belief in and adherence to those values. However, “doing” the right thing is not always enough. It is also important to avoid causing a perception of unethical behavior. The behavior of each and every individual in the organization, regardless of the level of authority, has an affect on others. If someone sees something they believe is wrong or unethical, then to that person, at least, it is reality. A perception of impropriety, correct or not, may be just as damaging as the real thing. For this reason, it is important

for every member of the organization to embrace and demonstrate the core values of the organization. Values, rules, and regulations should be communicated and demonstrated by the top levels of management to all staff members. Knowledge of and compliance with the organization's ethical standards help prevent accidental breaches, or the appearance of breaches. Ethical behavior by the organization's members can promote a culture of intolerance for unethical behavior. For this reason, communication and training rank high among the methods of ensuring an ethical environment. Respect, integrity, responsibility and accountability, and avoidance of conflicts of interest or commitment are among the cornerstones of ethical behavior. Ultimately, it is the responsibility of each individual to seek out and embrace the organization's core values and standards of conduct, monitoring their own actions to prevent even the

appearance of unethical behavior.



In the world of internal controls, ethical behavior sometimes is taken for granted. It shouldn't be. It is an ethical environment, produced by ethical behavior, that allows many internal controls to be effective at minimal cost. By minimizing temptation and confusion, internal controls help ethical people stay ethical. Conversely, breakdowns in ethical behavior lead to the circumvention of internal controls designed to minimize or prevent fraud, waste, and abuse. It is everyone's responsibility to behave ethically and promote ethical behavior within the organization.

Standards of Ethical Conduct for government employees may be found at: the United States Office of Government Ethics website: <http://www.usoge.gov/>

Taking Aim at Waste, Fraud, and Abuse

It's not a new concept. It is what the Chief Information Officer Managers' Internal Control Program is about, and has been since its inception. Internal controls, from the lowest level activities up,

are a major tool in preventing waste, fraud, and abuse. Whether assets are tangible (funds or property), or intangible (collective knowledge, databases, systems, licenses, to name a few),

the fundamental need for internal management controls is the same. The same goals and the same basic strategies apply. All carry risk. Internal controls de-

Continued on page 2

Taking Aim at Waste, Fraud, and Abuse *cont'd.*

signed to mitigate risk, including preventive and detective controls, are the tools commonly used. Audits, reviews, and formal reports such as the Annual Statement of Assurance are means of evaluating those controls.

Waste is the consumption or expenditure of resources without adequate return or benefit. Waste of effort, waste of time, and waste of supplies, all contribute in a very real way to the waste of resources.



Establishing and following policies; adhering to standard operating procedures (SOPs), including approval paths and the application of waste reduction methodologies; performing usage reviews such as billing official reviews; maintaining and/or tracking of intangibles are all useful in reducing and/or preventing waste. Relatively simple controls such as regulating access to supplies can go a long way towards preventing waste of expendables. Also consider:

- Print/copy using the double sided option.
- Use electronic copies instead of paper whenever possible.
- Buy recycled toner cartridges.
- Invest in rechargeable batteries and chargers.

True **Fraud** requires intent. Internal controls can not always prevent it, because a determined fraudster will find a way around them.



However, effective, well designed controls can detect fraud early and reduce its impact. “Accidental” fraud also happens, and it can be expensive. Accidental fraud, particularly in the area of contracting, may be the result of ignorance, or honest mistakes. Even so, it can result in damage to the organization and may be prosecutable, based on the “should have known” concept. In this area, internal controls can be extremely effective. Waste and abuse can be construed as accidental fraud, since they misdirect resources.

Approval paths, SOPs, system and personnel monitoring, reviews, internal audits, and training are among the more effective controls for detecting, preventing, and reducing both true fraud and accidental fraud. Also consider:

- Learn from the past.
- Base decisions on high quality evidence.
- Predict costs and then compare with actual costs.
- React to changing circumstances by keeping models current and procedures updated.

Abuse is the improper use of a resource through misapplication or other misuse. This sort of activity can end up being a topic in the evening news, and not in a good way. For example, in the last year several individuals have pleaded guilty and been sentenced for misuse of gov-

ernment property. Using government equipment to perform personal business, or “doing someone a favor” may seem harmless, but they are inappropriate uses of resources. They waste time and divert effort from legitimate, authorized activities.

Again, training, SOPs, and monitoring are among the more effective methods of internal control for prevention, detection, and mitigation of the risk of abuse. Also consider:

- Multiple approval requirement.
- Accurate office inventories of cell phones, laptops, and other big-ticket, easily-movable items.
- Periodic visual checks of office equipment.

Creating an environment in which appropriate information is freely available and communicated is also a major tool in preventing waste, abuse, and especially fraud. It is more difficult for any of these things to occur in a transparent environment. Fraud especially, requires an element of secrecy. Establishing clear lines of authority and communication within an office or organization facilitates the flow of information. An organizational chart demonstrating lines of communication is particularly useful.



It is never too late to take aim at waste, fraud, and abuse.

How Do You Rate Your Conduct on a Scale of 1-10?

- I make an effort not to waste supplies, time, or effort. _____
- I have a copy of the organization’s code or standard of conduct. _____
- I know who to contact if I suspect unethical behavior or wrongdoing. _____
- I would report unethical behavior, including waste, fraud, and abuse. _____
- I am careful in my conduct to avoid even the appearance of impropriety. _____

Be honest with yourself. No one is perfect.
You are your own best judge if improvement is needed.

Distance Doesn't Prevent Detection

An Alabama contractor and a U.S. Army contracting official and his wife, serving in Kuwait, have been indicted on multiple counts involving criminal monetary offenses. These offenses include bribery, wire services fraud, and money laundering conspiracy related to contracts for the delivery of bottled drinking water using two blanket purchase agreements (BPAs). The indictment alleges the contractor paid more than \$2.8 million in bribes to obtain the BPAs and

ensure the supply orders were directed to his company.

The contracting official and his wife are alleged to have received bribery payments using bank accounts set up in her name in Dubai, United Arab Emirates, and Cayman Islands. They are alleged to have devised "consulting agreements" for the purpose of creating the appearance that the bribes were legitimate earnings. The

government is seeking forfeiture of commercial real estate, residences, and expensive cars.

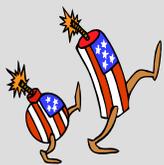


A U.S. Army Major, also a contracting official at the same camp in Kuwait, pleaded guilty to related charges. He is alleged to have received bribes totaling at least \$200,000 from the same contractor.

Source: www.usdoj.gov, 09-449 and 08-721

Assessable Unit Managers' Corner

Training for new MIC Program representatives will take place in July.



Representative refresher training will be available on the Managers' Internal Control Program page of the MHS CIO Website, <http://www.health.mil/mhscio/>, beginning FY 2010.



Timely Tip: Now and then, take time to document "lessons learned" along the way. They are a useful resource for the future and can help prevent making the same mistake twice.



Audit Reviews Highlight Internal Control

Due to the persistent nature of information security vulnerabilities and the associated risks, GAO continues to designate information security as a government-wide high-risk issue in its most recent biennial report to Congress, a designation it has made in each report since 1997. Significant weaknesses in information security policies and practices expose sensitive data to significant risk, as illustrated by recent incidents at various agencies. GAO audits and reviews by inspectors general note significant information security control deficiencies that place agency operations and assets at risk. In their fiscal year 2008 performance and accountability reports, 20 of 24 major agencies noted that the information system controls over their financial systems and information were either a significant deficiency or a material weakness. An underlying cause for information security weaknesses, identified at federal agencies, is that they have not yet fully or effectively implemented key elements for an agency-wide information security program, as required by FISMA. Twenty-three of the 24 major federal agencies had weaknesses in their agency-wide information security programs. To read more about this report (GAO-09-701T), please visit www.gao.gov/new.items/d09701t.pdf.

The Securities and Exchange Commission (SEC) has made important progress toward correcting previously reported information security control weaknesses. It has corrected or mitigated 18 of 34 previously reported weaknesses. However, SEC has not completed actions to correct the remaining 16 previously reported weaknesses. In addition, GAO identified 23 new weaknesses in controls intended to restrict access to data and systems. Also, weaknesses in other information security controls continue to jeopardize the confidentiality, integrity, and availability of SEC's financial and sensitive information and information systems. The commission has not fully implemented effective controls over access to computing resources, and did not consistently ensure appropriate segregation of incompatible duties or adequately manage the configuration of its financial information systems. To read more about this report (GAO-09-203), please visit <http://www.gao.gov/new.items/d09203.pdf>.



"It is not what we do, but also what we do not do, for which we are accountable."

~ Molière