



Chief Information Officer Managers' Internal Control Program



INFORMATION BULLETIN

Volume 7, Issue 4

September 27, 2010

Special Message:

Happy New Year!

OK, it's not the middle of winter, but it is the beginning of the new fiscal year. Now is a great time to make resolutions to improve controls in your area. Start by reviewing and updating policies, procedures, and processes to ensure a fantastic year.



Management is responsible for establishing specific internal control policies and procedures and employees are responsible for ensuring that internal controls are followed and applied.



OMG, Where's My Laptop!

Your government furnished computer (or other expensive equipment) is missing. Now what?! What you do next depends on the circumstances. Was it stolen, or just misplaced?

If theft is a certainty, for instance from your car, home, or hotel room, call the police and then your immediate supervisor. You will need a police report/case number to furnish to your security officer, Helpdesk, and your insurance provider if appropriate.

If you are at work, first check with your supervisor and co-workers to see if the equipment is missing for a legitimate reason. In the case of theft, a police report must still be filed, but your office's security procedure determines who makes the call.

If theft is not clearly indicated, for instance it disappeared during an office move and may only be misplaced, notify your supervisor but **don't** call the police. In the event the equipment remains missing, notify your security officer, Helpdesk or other

authority designated in the security procedures for your Division/Program Office or office suite. They will tell you what to do next, and provide you with any forms you may need.

In either case, if personal health information (PHI) and/or personally identifiable information (PII) is located on the missing computer it is vital that your security officer (or other appropriate authority) and Helpdesk are informed at the start. Above all, do not sit on this information. Bad news does not improve with time.

If you are contractor personnel, the Contracting Officer's Representative (COR) in charge of your contract will also need notification. Unless otherwise directed, your contract lead or manager ensures that the COR is notified.

Whether you are government or contractor, follow established procedures for your organization. Once you have notified the appropriate authority, wait for instructions on next steps. Regardless of the reason the equipment is

missing there will be an investigation of one sort or another. In instances where negligence is involved, or if insurance will reimburse all or part of the value, it is highly likely the government will expect reimbursement for the loss.



Using good sense and practicing established security protocols will prevent most losses. Don't leave your laptop or other equipment unsecured. Locks are a good deterrent in most cases. If you must leave your laptop, video camera or other attractive, easily portable items in your vehicle or hotel room, don't tempt fate by leaving them in plain sight.

Be safe, not sorry, and be proactive. Make a point of knowing who you should contact if necessary. Familiarize yourself with the security procedures specific to your situation/location. Ultimately, you are responsible for the government furnished equipment you use.

Where's the Risk? – Everywhere!

The need to manage (prevent or mitigate) risk should be the primary driving force behind the development and implementation of internal controls at every level. Once Assessable Units (AUs) and their associated functions and activities are reviewed and updated, the very next step is to assess the risks to those AUs, functions, and activities. Then control measures can be developed and/or applied.

Identifying Risks - Don't forget BRAC risks!

When you conduct your annual risk assessment be sure to consider the potential risks which could occur when relocating your organization. Consider the following as you identify and assess your risks:



- Accuracy of your equipment inventory
- Currency of your file plan and status of your identification of documents to move or store
- Reviewing processes to determine risk of workflow interruption
- Ability to receive and take action on HA/TMA transition information in a timely manner

Identifying BRAC risks and incorporating them in your CIO MICP Risk Assessment, due not later than December 30, 2010, helps prevent ineffective use of government resources. Developing and applying effective controls for identified risks helps ensure your office makes the move successfully, with a minimum of disruption to achievement of mission objectives.

Effective Internal Controls

From *Internal Control News*, June 2010, Vermont Department of Finance and Management, comes this good advice:

Understanding some of the most significant threats to the effectiveness of internal controls can help management assess/develop effective internal controls, taking proactive steps to minimize risk and exposure to loss. Among the most important things to consider when developing or assessing internal controls:

- **Failure to Anticipate Risks:** Management's inaction or inability to anticipate certain risks may result in a failure to design and implement appropriate controls.
- **Form over Substance:** Controls may appear to be well-designed but still lack substance (e.g., written procedures that aren't followed, flow charts that don't accurately depict the actual process, lackadaisical approval of documents).
- **Management Override:** Management's capability to overrule or circumvent prescribed policies or procedures for illegitimate purposes – such as an enhanced presentation of an organization's financial condition or compliance status, or for personal gain.
- **Conflict of Interest:** When an employee's loyalties are divided and/or personal financial gain is at stake, there is a distinct risk an employee will choose a course of action detrimental to the organization.
- **Access to Assets:** Unfettered access to assets (physical assets, cash, confidential data, etc.) increases the risk of misappropriation, theft, misuse, and abuse. Access restrictions, based on legitimate and authorized need minimize this threat.
- **Collusion:** Two or more individuals can conspire to perpetrate and conceal an action, altering financial data or other management information in a manner that circumvents controls and avoids detection.

The Whole Truth And Nothing But The Truth Will Do

A former U.S. Army contracting official faces a maximum of 5 years in prison and a \$250,000 fine according to an announcement by Department of Justice released September 2, 2010. William T. Armstrong, former chief of construction at the Fort Carson Construction Directorate, pleaded guilty to submitting a **false statement** to the U.S. Army. In addition to the statutory maximum, there is provision for the fine to increase

to twice the gain derived from the crime, or twice the loss suffered by victims of the crime, if either of those amounts exceeds 250 thousand dollars.

The one-count felony charge filed in July this year against Armstrong stemmed from providing false information on an annual confidential financial disclosure report submitted to the U.S. Army Contracting Agency. In his 2008

report Armstrong denied receiving "reportable gifts" during the previous year, when in fact he received several thousand dollars worth of gifts from a construction contractor that had substantial business with the Fort Carson Directorate of Contracting.

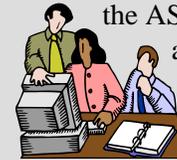
To read more, please visit: http://www.justice.gov/atr/public/press_releases/2010/262161.pdf

Assessable Unit Managers' Corner

Please give special attention to the FY11 CIO MICP activities coming up this fall and winter. Remember, they contribute to the Annual Statement of Assurance (ASA) next spring, providing you with trackable, reportable data.

- **CIO MICP Annual Training on MHS Learn: Oct. 1 - Dec. 17**
- **Review/Update Assessable Unit, Functions & Activities and Activity POCs: Oct. 15 - Nov. 30**
- **Revalidate/Perform Risk Assessments: Nov. 1 - Dec. 30**
- **Self Assessment Review: Dec. 1 - Feb. 28**

There is a requirement that an audit trail be available if requested for all data reported in the ASA. A little extra



attention when performing these activities will make reporting relevant data in the ASA much easier.

Audit Reviews Highlight Internal Control

July 1, 2010: GAO identified several significant internal control system weaknesses that have been present at Joint Improvised Explosive Device Defeat Organization (JIEDDO) since GAO's first review in 2007. Beyond those identified in the most recent report, weaknesses extend to other areas such as financial and human capital management. Although JIEDDO has taken some steps in the past to address these weaknesses, those efforts have not been successful. According to federal standards, internal control is a major part of managing an organization. Some underlying reasons for JIEDDO's lack of progress in addressing these weaknesses include a lack of sustained management attention in following through with corrective actions; challenges with retention and expertise of personnel; and a lack of sufficient acquisition expertise with breadth and depth to understand the programs. To read more about this report (GAO-10-660), please visit <http://www.gao.gov/new.items/d10660.pdf>.

Historically, different information security policies and guidance governed civilian and national security-related information technology (IT) systems. Asked to assess the progress of federal efforts to harmonize policies and guidance for these two types of systems, GAO reviewed program plans and schedules, analyzed policies and guidance, assessed program efforts against key practices for cross-agency collaboration, and interviewed officials responsible for this effort. While progress has been made, additional work remains. DOD and the intelligence community are developing agency-specific guidance and transition plans for implementing harmonized guidance, but actual implementation could take several years to complete. In a report released in July, GAO recommended that the Secretary of Commerce and the Secretary of Defense, among other things, update plans for future collaboration, establish timelines for implementing revised guidance, and fully implement key practices for interagency collaboration in the harmonization effort. To read more about this report (GAO-10-916), please visit <http://www.gao.gov/new.items/d10916.pdf> <http://www.gao.gov/new.items/d10916.pdf>.



Special Notice

October 1, 2010:

CIO Managers' Internal Control Program Annual Training provided through MHS Learn now compliant with Section 508 of the Rehabilitation Act of 1973.