



Chief Information Officer Managers' Internal Control Program



INFORMATION BULLETIN

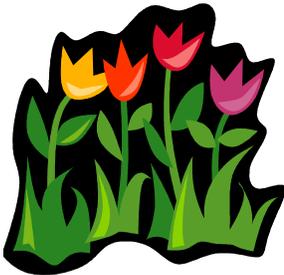
Volume 5, Issue 2

April 9, 2008

Special Message:

Spring is here and development of the Annual Statement of Assurance report is in full swing. Assessable Unit (AU) Managers should take special note of the AU Managers' Corner on page 3 identifying responsibilities associated with this report.

SPRING



"When we improve our processes, we improve everything we do every day so that we can better invest the resources that the taxpayers provide us for our national defense and our security." Secretary England

Continuous Process Improvement Lean Six Sigma

Have you heard of Lean Six Sigma? If not, you will! Deputy Secretary of Defense Gordon England has announced that Lean Six Sigma (LSS) will be the framework of DoD's continuous process improvement initiative. LSS is a best practice/proven methodology that couples a disciplined approach to **continuous process improvement** with a strong focus on **delivering value to the customer**.

According to Elizabeth McGrath, Principal Deputy Under Secretary of Defense for Business Transformation, "Lean Six Sigma provides a framework through which complicated processes can be examined in an organized and understandable way, thereby allowing us to identify where specific inefficiencies reside and allowing us to fix them."

The process improvements that the Department is working to achieve are first and foremost those that support the warfighter. LSS has been endorsed by DoD leadership as the means by



which the Department will become more efficient in its operations and more effective in its support of the warfighter.

In May 2006, Secretary England established a DoD-wide Continuous Process Improvement (CPI) Program to improve the operational, administrative, and support functions across the department. By April 2007, the overall success of this effort, combined with the successes of LSS in the Military Services, led Secretary England to establish the CPI/LSS Program Office to expand its use throughout DoD.

CPI/LSS is rapidly becoming embedded in the DoD culture, as it is a critical component to efficient use of taxpayer dollars and support to the warfighter.

"The Secretary and I expect that every DoD organization is focused every day on improving the effectiveness of our support to the Warfighter,"

said Deputy Secretary of Defense Gordon England.



The industry's standard principles of LSS are an integral part of DoD's continuous process improvement effort. By focusing on becoming a "lean" organization, DoD can address resource constraints and other barriers to improving business performance by eliminating waste and defects that hinder operational excellence. The DoD organization will benefit from better quality, faster turnaround, lower costs, and more responsive service.

To learn more about LSS, the following free courses are available online through the DAU (<https://learn.dau.mil/>):

1. Introduction to Lean Enterprise Concepts ([CLE 004](#)),
2. Lean-Six Sigma ([CLE 007](#)), and
3. Six Sigma: Concepts and Processes ([CLE 008](#)).

Best Practices for Protecting Government Information

The Office of Management and Budget (OMB) and the Department of Homeland Security (DHS) have identified 10 common risks impeding the adequate protection of government information and their associated best practices to help agencies mitigate and avoid these risks. Below is an extract of this publication.

Risk:

- 1 Security and privacy training is inadequate and poorly aligned with the different roles and responsibilities of various personnel.

Best Practices/Internal Controls:

- Agencies provide security and privacy training for all personnel upon hiring and at least annually. Both initial and refresher training explain acceptable rules of behavior and the consequences when rules are not followed.
- Agencies use creative methods to promote daily awareness of employees' privacy and security responsibilities, such as providing weekly tips, annual "security days," frequently asked questions, mouse pads imprinted with security reminders, privacy screens when using laptops in public, and incentives for reporting security risks.

Risk:

- 2 Contracts and data sharing agreements between agencies do not describe the procedures for appropriately processing and adequately safeguarding information.

Best Practices/Internal Controls:

- Agencies establish contracts and agreements describing the procedures for appropriately using and adequately protecting information, and identify who is responsible for ensuring the procedures are completed.
- Agencies incorporate standardized Federal Acquisition Regulation

(FAR) language when developing contracts and agreements.

Risk:

- 3 Information inventories inaccurately describe the types and uses of government information, and the locations where it is stored, processed or transmitted, including personally identifiable information.



Risk:

- Agencies report suspicious activities and incidents in a timely manner to mitigate harm and prevent similar incidents from re-occurring.
- 6 Audit trails documenting how information is processed are not appropriately created or reviewed.

Best Practices/Internal Controls:

- Agencies use their enterprise architectures and inventories of information collections to maintain an understanding of the types and uses of information collected and processed at their agency, and to ensure information is used to support the proper performance of agency function.
- Agencies use inventory when determining which security controls are necessary to adequately secure information.

Risk:

- 4 Information is not appropriately scheduled, archived, or destroyed.

Best Practices/Internal Controls:

- Agencies obtain the National Archives and Records Administration's approval for the disposition of their information holdings by establishing record schedules, as required by 44 U.S.C. 3303.
- Agencies use these record schedules to determine how long information needs to be maintained, and whether it needs to be archived or can be destroyed.

Risk:

- 5 Suspicious activities and incidents are not identified and reported in a timely manner.

Best Practices/Internal Controls:

- Agencies develop and implement standard operating procedures describing how to identify and report

suspicious activities and incidents.

- Agencies report suspicious activities and incidents in a timely manner to mitigate harm and prevent similar incidents from re-occurring.

Best Practices/Internal Controls:

- Agencies log all computer-readable data extracts from databases holding sensitive information and verify each extract, including whether sensitive data has been erased within 90 days or its use is still required.
- Agencies use information provided by audit trails to identify anomalies in accessing information and determine whether information is no longer needed for the proper performance of agency function.

Risk:

- 7 Inadequate physical security controls where information is collected, created, processed or maintained.

Best Practices/Internal Controls:

- Agencies maintain an accurate inventory of their portable and mobile devices.
- Agencies locate where high-impact and high-risk information systems operate, and apply commensurate controls to mitigate risk.

Risk:

- 8 Information security controls are not adequate.

Best Practices/Internal Controls:

- Security controls are tested regularly, and at least annually, to ensure they are effective.

Continued on next page

Best Practices for Protecting Government Information Cont'd

- Agencies share the results from control testing quickly with those who need to improve them.

Risk:

- ⑨ Inadequate protection of information accessed or processed remotely.

Best Practices/Internal Controls:

- Agencies develop and implement telework policies describing procedures personnel must take to securely access government information remotely.
- Agencies maintain an audit log of

information accessed or processed remotely, as appropriate.

Risk:

- ⑩ Agencies acquire information technology and information security products without incorporating appropriate security and privacy standards and guidelines.

Best Practices/Internal Controls:

- Agencies incorporate the costs for security and privacy in their information technology investments and throughout the system development

life-cycle, including information system planning, development and maintenance.

- Agencies acquire IT products incorporating information security and privacy requirements, as appropriate.

For a complete copy of this publication please visit <http://csrc.nist.gov/pcig/document/Common-Risks-Impeding-Adequate-Protection-Govt-Info.pdf>.

Assessable Unit Managers' Corner

Every year the MHS CIO is required to submit an Annual Statement of Assurance (ASA) report, as required by Congress, documenting whether there is reasonable assurance that the organization's internal controls are achieving their intended objectives. This ASA report addresses the evaluation of the CIO MIC Program and represents the CIO's informed

judgment as to the overall adequacy and effectiveness of internal control within the organization.

The CIO's judgment is based solely on the ASA input received from the OCIO Divisions/Offices. As such, the Assessable Unit (AU) Manager for each division/office must en-



sure that all ASA (TAB A) questions are appropriately addressed and that their input is comprehensive, timely, and accurate. Although the date for the draft ASA input has passed, AU Managers may continue to provide additional input until April 15.

Audit Reviews Highlight Internal Control

During their review of agencies' progress in developing policies and procedures on the protection of personally identifiable information (PII), the GAO found that not all agencies have developed the range of policies required by OMB. Twenty-two of the 24 agencies reviewed had developed policies requiring encryption of PII on mobile devices and computers. However, when it came to agencies with policies addressing OMB's other protection recommendations, the numbers were significantly smaller. GAO also reiterated that "although having specific policies and procedures in place is an important factor in helping agencies to secure their information systems and to protect personally identifiable information, **proper implementation of these policies and procedures remains crucial.**" To read more about this report (GAO-08-343), please visit http://www.health.mil/mhscio/Man_Ctrl_Prog_Audits.htm.

During their review on Contractor Past Performance Information, the DoD IG found that the DoD Contractor Performance Assessment Reporting System (CPARS) did not contain all active system contracts over \$5 million. In addition, for the system contracts that were in CPARS, the IG found that: 39% were registered over a year late; 68% had performance reports that were overdue; and 82% of the past performance reports did not contain detailed, sufficient narratives to establish that ratings were credible and justifiable. According to the IG, this occurred due to a **lack of OSD and Military Department emphasis and guidance** on timely registration of contracts in CPARS, accurate and timely reporting of past performance in CPARS, and training for past performance assessment report preparation. To read more about this report (D-2008-057), please visit http://www.health.mil/mhscio/Man_Ctrl_Prog_Audits.htm.



"As the federal government obtains and processes information about individuals in increasingly diverse ways, it is critically important that it ensure that the privacy rights of individuals are respected and this information is properly secured and protected."