OFFICE OF THE UNDER SECRETARY OF DEFENSE
1100 DEFENSE PENTAGON
WASHINGTON, DC 20301-1100

COMPTROLLER

DEC 19 2016

MEMORANDUM FOR DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
DIRECTOR, DEFENSE LOGISTICS AGENCY
DIRECTOR, DEFENSE FINANCE AND ACCOUNTING SERVICE
DIRECTOR, DEFENSE CONTRACT MANAGEMENT AGENCY
DIRECTOR, DEFENSE HUMAN RESOURCES ACTIVITY
DIRECTOR, ACQUISITION RESOURCES AND ANALYSIS, OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS

SUBJECT: Addressing Requirements of American Institute of Certified Public Accountants New Standards for Service Organization Control Reports

The Department of Defense (DoD) has made significant investments in the audit readiness of service organizations, including preparing for, and obtaining Service Organization Control reports (SOC 1 reports) performed in accordance with Standards for Attestation Engagements Number 16 (SSAE No. 16) and the associated Attestation Standard 801 (AT 801). These reports provide auditors independent assurance on service organization controls likely to be relevant to reporting entities' internal controls over financial reporting.

In April 2016, the American Institute of Certified Public Accountants (AICPA) released Standards for Attestation Engagements Number 18 (SSAE No. 18), clarified Attestation Standards AT-C 320 (Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting), AT-C 105 (Concepts Common to All Attestation Engagements), and AT-C 205 (Examination Engagements) which supersede SSAE No. 16 and AT 801 for service auditor reports issued after April 30, 2017.

Since the SOC 1 reports issued by DoD service organizations (and subservice organizations) are aligned to the Department's fiscal year reporting period, they are all impacted by these new standards effective in fiscal year (FY) 2017. Attached are the requirements to be implemented for the FY 2017 (and subsequent) SSAE 18/ATC-320 examinations. Please provide periodic updates at the service provider working group meetings to the Financial Improvement and Audit Readiness Directorate (FIAR) on your progress.

In addition, to enhance auditor reliance on the SOC 1 reports, the scope in existing reports need to be expanded (or new SOC 1 reports added) to provide more comprehensive coverage of the full processes. Accordingly, please provide to the FIAR Directorate, by February 28, 2017, a plan for expanding existing report's scope and adding new SOC 1 reports. The plans should include milestones and expected milestone completion dates.

My staff POC is Mr. James Davila. He can be reached at (703) 571-1654 or james.r.davila2.civ@mail.mil.

Mark E. Easton
Deputy Chief Financial Officer

Attachment:
As stated

cc:
Under Secretary of Defense for Acquisition, Technology, and Logistics
Under Secretary of Defense for Personnel and Readiness
Deputy Chief Management Officer
Assistant Secretaries of the Military Departments (Financial Management and Comptroller)
Directors of the Defense Agencies
Directors of the DoD Field Activities
Deputy Inspector General for Auditing, DoD Office of Inspector General

Seven Requirements of AICPA New Standards for Service Organization Control Reports

The following summarizes actions required to successfully prepare for the SSAE 18 / ATC-320 examinations (for service auditor reports issued after April 30, 2017) and changes required to the SOC 1 reports to allow for standardization and consistency across DoD service organizations. These actions will promote reliance on the SOC 1 reports by reporting entity auditors. It is critical that service organizations and subservice organizations partner and communicate regularly to fully implement the revised standard initially and each year thereafter. To the extent possible, individual requirement milestone dates have been provided as a guide for implementation.

For Service Organizations.

1. Service organization management will conduct a meeting with the IPA (Independent Public Accountant) performing the SSAE 18 / AT-C 320 examination (the service auditor), prior to January 13, 2017, to establish an understanding of the service auditor's interpretation of requirements introduced by the new standards and associated changes to the SOC 1 reports.

2. Service organization management will validate the reliability of its internally-produced reports and data used to support its internal controls. Service organization management will also validate reports and data provided to user entities that support their internal controls over financial reporting including Complementary User Entity Controls (CUECs) defined in the scope of the SSAE 18 / AT-C 320 examination.

3. For subservice organizations identified in the service organization SSAE 18 / AT-C 320 examination, service organization management will prepare written descriptions of Complementary Subservice Organization Controls (CSOCs). These are the controls that were designed to achieve the control objectives included in the scope of the service organization SSAE 18 / AT-C 320 examination. These CSOCs are to be aligned to service organization control objectives and incorporated into section 3 of the service organization SOC 1 reports (to appear after the CUEC section in a section labelled "Complementary Subservice Organization Controls" under the main heading of "Subservice Organizations" after the subservice organizations have been listed). To assist with documenting the CSOCs, a CSOC identification template was developed and is located on the FIAR Director website at the following web address:

   http://comptroller.defense.gov/fiar/fiarguidance/tools_tips_workproducts.aspx#service-phase5. File name (Complementary Subservice Organization Controls Identification Workbook)

4. For each CSOC identified for inclusion in the Service Organization's SOC 1 report, service organization management will document the following for the related assertion:

   a. The basis / rationale for concluding the Subservice Organization performs the CSOC on behalf of the Service Organization for the systems and/or processes included in the scope

of the SSAE 18 / AT-C 320 examination. This may include, but not be limited to, terms of service level agreements, memos of understanding, and catalog(s) of services, etc.

b. Monitoring controls over the subservice organization that service organization management has established to determine if the CSOCs are designed and operating effectively. This may include, but not be limited to:

   i. obtaining and reviewing the subservice organization SOC 1 reports,

   ii. reviewing and reconciling reports / data provided by the subservice organizations to include those related to their performance,

   iii. periodic review and update of service level agreements,

   iv. holding periodic discussions with the subservice organization,

   v. making regular site visits to the subservice organizations,

   vi. testing controls at the subservice organization by members of the service organization's internal audit function, and

   vii. monitoring external communications, such as customer complaints relevant to the services by the subservice organization, etc.

5. Service organization management will provide the identified CSOCs to each impacted subservice organization no later than January 23, 2017.

For Subservice Organizations.

6. Within fourteen business days of receiving the identified CSOCs, the subservice organization will confirm that the CSOCs are in place and operating as described and will be incorporated into the Subservice Organization SOC 1 report. In addition, the subservice organization will provide notification to the service organizations of instances where controls are not in place or do not plan to implement controls to address the CSOCs.

7. In instances where controls are not in place at the subservice organization or remediation activities are being performed to implement the control, subservice organization management will provide a corrective action plan to the impacted service organizations no later than twenty-one business days after receiving the identified CSOC. This corrective action plan will, at a minimum, describe the control to be implemented and the expected implementation date. Where applicable, the corrective action plan will also identify the first SOC 1 examination period expected to include the additional control.