**INSPECTOR GENERAL**
**DEPARTMENT OF DEFENSE**
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

February 10, 2015

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS
ASSISTANT SECRETARY OF THE AIR FORCE (FINANCIAL MANAGEMENT AND COMPTROLLER)
DOD CHIEF INFORMATION OFFICER
DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR SYSTEMS ENGINEERING
NAVAL INSPECTOR GENERAL
AUDITOR GENERAL, DEPARTMENT OF THE ARMY

SUBJECT: Audit of Software Assurance in DoD Programs
(Project No. D2015-D000RB-0125.000)

We plan to begin the subject audit in February 2015. This is the first in a series of audits on software assurance. Our objective is to determine whether critical software components for selected Acquisition Category I programs received the required software assurance testing to reduce the risk of vulnerabilities in operational software. We will consider suggestions from management on additional or revised objectives.

We will perform the audit at the Offices of the Under Secretary of Defense for Acquisition, Technology, and Logistics, the DoD Chief Information Officer, and selected Military Service activities. We may identify additional locations during the audit.

Please provide us with a point of contact for the audit within **10 days** of the date of this memorandum. The point of contact should be a Government employee—a GS-15, pay band equivalent, or the military equivalent. Send the contact's name, title, grade/pay band, phone number, and e-mail address to audrco@dodig.mil.

You can obtain information about the Department of Defense Office of Inspector General from DoD Directive 5106.01, "Inspector General of the Department of Defense (IG DoD)," April 20, 2012; DoD Instruction 7600.02, "Audit Policies," October 16, 2014; and DoD Instruction 7050.03, "Office of the Inspector General of the Department of Defense Access to Records and Information," March 22, 2013. Our website is www.dodig.mil.

If you have any questions, please contact [redacted]

Carol N. Gorman
Assistant Inspector General
Readiness and Cyber Operations