SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

MAR 18 2014

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
CHIEFS OF THE MILITARY SERVICES
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANT SECRETARY OF DEFENSE FOR LEGISLATIVE AFFAIRS
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER
ASSISTANT TO THE SECRETARY OF DEFENSE FOR PUBLIC AFFAIRS
DIRECTOR, ADMINISTRATION AND MANAGEMENT

SUBJECT: Final Recommendations of the Washington Navy Yard Shooting Internal and Independent Reviews

Following the tragic shooting at the Washington Navy Yard on September 16, 2013, I directed concurrent Internal and Independent Reviews to identify and recommend actions to address any gaps or deficiencies in DoD programs, policies, and procedures regarding security at DoD installations and the granting and renewing of security clearances for DoD and contractor personnel. The reviews considered previous relevant studies in arriving at their conclusions.

After considering the findings and recommendations from the reviews, I approve the following four key recommendations, as well as the way ahead described in the attachment. I have also directed the Under Secretary of Defense for Intelligence (USD(I)) to conduct further analysis of three additional recommendations developed by the Independent Review (attached).

Four Key Recommendations:

1. Implement Continuous Evaluation. Implement continuous evaluation in coordination with the Office of the Director of National Intelligence and the Office of Personnel Management, as appropriate, to provide automated records checks of personnel with access to DoD facilities or classified information.

2. Establish a DoD Insider Threat Management and Analysis Center (DITMAC). Establish a DITMAC with assigned cross-functional representatives to assess, recommend intervention or mitigation, and oversee case action on threats that insiders may pose to their colleagues and/or DoD missions and resources. With regard to the

protection of classified networks and information, the DITMAC would also fulfill certain requirements of the National Insider Threat Policy and Minimum Standards.

3. Centralize Authority, Accountability and Programmatic Integration Under a Single Principal Staff Assistant (PSA). Centralize authority, accountability and programmatic integration of continuous evaluation and establishment of the DITMAC under the USD(I) as the PSA with fiscal control over the Department's personnel security resources.

4. Resource and Expedite Deployment of the Identity Management Enterprise Services Architecture (IMESA). Examine resourcing the deployment of IMESA in FY 2016.

Leaders at every level play a critical role in ensuring the security of our workforce. The Department will empower military and civilian leaders with the tools and discretion they need to take appropriate action consistent with law and policy to prevent and respond to potential insider threat problems, whatever their cause.

I hereby direct USD(I) to lead a task force to develop and coordinate an implementation plan, based on the above listed key recommendations, for my approval, and for all DoD components to support this task force. During the development of the implementation plan, the task force will consult with the DoD General Counsel, as well as civil liberties and privacy officials, to ensure legal and privacy issues are appropriately identified and addressed.

Attachments:
As stated