

ACTION MEMO

PDUSD(P) My
JAN 19 2017

FOR: DEPUTY SECRETARY OF DEFENSE

FROM: Tom Atkin, Acting Assistant Secretary of Defense for Homeland Defense and Global Security

JAN 19 2017

SUBJECT: Close Out of Actions Directed in Response to Fort Hood Recommendations: Capabilities for Managing the Risk from Violent Behavior and Similar Threats

- (U) Request you sign the memorandum at TAB A, instructing Components to implement the final four SecDef directed actions in response to the tragic shooting at Fort Hood in November 2009, and also task the USD(I) to develop a proposal for combining the Prevention, Assistance, and Response (PAR) capabilities construct and the DoD Insider Threat Program into one coherent program.
 - The Mission Assurance Coordination Board (MACB) will monitor implementation, take appropriate actions, and make recommendations as needed.
- (U) The memorandum's guidance on PAR capabilities comprehensively addresses and closes out the four remaining actions by directing the synchronization of existing efforts as follows:
 - (U) **Recommended Action:** Develop a risk assessment tool for commanders, supervisors, and professional support service providers to determine whether and when DoD personnel present risks for various types of potentially violent behavior. ✓
 - (U) The memorandum directs DoD Component heads to synchronize existing personnel support programs and processes into a comprehensive effort, using existing professionally trained personnel to serve as functional experts to provide input to commanders and their equivalent civilian leaders to enable them to develop a risk assessment and implement informed decisions to manage the risk from potentially violent behavior.
 - (U) Rather than a physical or automated tool, we think using this process is the most practicable means of meeting this requirement. We recommend that you approve using this process to assist commanders and close the recommendation. This approach has concurrence from relevant Principal Staff Assistants and the Secretaries of the Military Departments.
 - (U) The memorandum directs the Under Secretary of Defense for Policy to coordinate with other OSD Component heads to evaluate studies on violent behavior, and any risk management tools these studies identify, as aids to DoD Component heads in an effort to develop improved decision support tools for commanders and equivalent civilian leaders.

Prepared by: Larry Turner, OASD(HD&GS), DCMA, AT Policy, 571-256-9173



| | | | |
|--------|--------|---------|----------|
| SD CA | | DSD SA | |
| SD SMA | | DSD SMA | |
| SD MA | | DSD MA | BWB 1/24 |
| TSA | | DSD CA | |
| SA | | | |
| ES | | ESB Rvw | BS 1/24 |
| ESR | R 1/23 | ESD | ✓ |



UNCLASSIFIED


- (U) The memorandum lists numerous indicators of potentially violent behavior. It assigns responsibilities to DoD Component heads to train DoD military personnel, civilian employees, and defense contractor personnel to recognize and to report those indicators.
- (U) **Recommended Action:** Ensure that the DoD Components establish implementing guidance for multi-disciplined threat management capabilities. ✓
- (U) The memorandum prescribes minimum operating standards for PAR capabilities through synchronizing and leveraging the network of existing support functions.
- (U) **Recommended Action:** Establish minimum procedures and mechanisms for sharing communications on potentially violent behaviors across the Components' threat management capabilities. ✓
- (U) The memorandum prescribes procedures on how DoD Components will use the PAR capabilities construct to coordinate the sharing of information on personnel at risk of potentially violent behavior between installation and organizational commanders and the DoD Component Insider Threat Hubs.
- (U) **Recommended Action:** Incorporate threat management information sharing procedures into policy. ✓
- (U) The memorandum assigns responsibilities to OSD Principal Staff Assistants to update existing DoD policies on workforce violence, insider threats, antiterrorism, and contractor personnel requirements to ensure that they are cohesive and mutually supporting.
- (U) The PAR capabilities concept does not create new capabilities or organizations, but instead directs DoD Component heads to establish procedures to identify and assign functional experts within existing support functions. The experts will network and synchronize these functions, and make them available to all installation and organizational commanders as an aid in providing assistance to their personnel at risk for potentially violent behavior.
- (U) The memorandum provides for the synchronization of these existing efforts at the installation level with those at the DoD Component Hubs, and closing of any remaining gaps in guidance on risk management of potentially violent behavior.
- (U) The memorandum has been coordinated at the Principal level and all comments adjudicated. The Navy recommended that we include definitions for three terms: event, incident, and indicator. We were not able to develop these definitions however, as after thorough coordination with the Office of the General Counsel, we realized the definitions for these commonly used words as they pertain to this memorandum induced more vagueness and ambiguity and would add no value. ✓
- (U) In addition, the FY 2017 National Defense Authorization Act (NDAA) expansion of the statutory definition of insider threats provides an opportunity to combine the PAR capabilities with the existing USD(I)-run DoD Insider Threat Program. In addition to the

UNCLASSIFIED

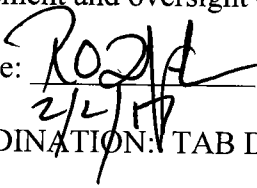
DoD Insider Threat program, the DoD Components have taken a range of actions to address insider threats (TAB B).

- (U) The Office of the General Counsel reviewed the memorandum and has found it legally sufficient (TAB C).

RECOMMENDATION 1: Sign the memorandum at TAB A.

Approve:  Disapprove: _____ Other: _____

RECOMMENDATION 2: Task the USD(I) to develop a proposal for combining the PAR capabilities construct and the DoD Insider Threat Program into one coherent program, under the management and oversight of the USD(I), within 12 months.

Approve:  Disapprove: _____ Other: _____

COORDINATION: TAB D

Attachments:

TAB A: PAR Capabilities Memorandum

TAB B: Service Approaches to Insider Threat and Workplace Violence

TAB C: Legal sufficiency statement

TAB D: Coordination

TAB

A



**DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010**

FEB 02 2017

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
CHIEF OF THE NATIONAL GUARD BUREAU
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER
ASSISTANT SECRETARY OF DEFENSE FOR LEGISLATIVE
AFFAIRS
ASSISTANT TO THE SECRETARY OF DEFENSE FOR PUBLIC
AFFAIRS
DIRECTOR OF NET ASSESSMENT
DIRECTOR, STRATEGIC CAPABILITIES OFFICE
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Final Implementation Actions of Fort Hood Recommendations: Managing Risk of Potentially Violent Behavior through Prevention, Assistance, and Response Capabilities

This memorandum and its attachments establish policy, prescribe procedures, and assign responsibilities for implementing prevention, assistance, and response (PAR) capabilities. PAR capabilities will provide commanders and their equivalent civilian leaders with options to care for their personnel at risk of potentially violent behavior and address their areas of concern, regardless of whether or not those personnel have at any time been granted eligibility for access to classified information or eligibility to hold a sensitive position.

DoD Component heads will implement this policy immediately and will establish procedures to identify and assign existing professionally trained and qualified personnel within existing support functions to serve as PAR functional experts. The experts are to be made available to all installation commanders and their equivalent civilian leaders.

DoD Component heads that have already established PAR-like support capabilities are not required to establish new PAR-like capabilities, but the established capabilities must meet the intent of this memorandum. DoD Component heads that have not already established PAR-like capabilities must determine how best to use their existing capabilities to meet the intent of this memorandum. In either case, all DoD Component heads must report to the Mission Assurance Coordination Board (MACB) as to how they are meeting the intent of this memorandum.



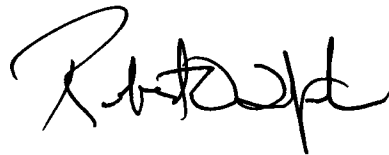
OSD000608-17/CMD000828-17

The PAR capabilities concept requires that DoD Component heads establish procedures to: 1) identify and assign existing personnel within existing support functions (an example list is in paragraph 3.d. of Attachment 3) to serve as functional experts; 2) to ensure that these experts network with one another to synchronize their support functions; 3) to ensure that the support functions are available to the installation and organizational commanders and their equivalent civilian leaders; and 4) to ensure that these experts provide input to their commander's or equivalent civilian leader's risk assessments to aid leaders in developing options to stop violent behavior, to protect those at risk, and to provide assistance to personnel at risk for potentially violent behavior. Implementing these tasks ensures that leaders have a consistent process available to them to identify, assess, and manage the risk of violent behavior for all DoD military and civilian personnel and defense contractor personnel

The PAR capabilities concept is intended to utilize existing capabilities to the maximum extent possible. So long as the functional capabilities discussed in this memo are available to commanders and their equivalent civilian leaders, there is no requirement to create any new capability. Likewise, there is no requirement to duplicate any existing capability. The PAR capabilities concept relies on maintaining case-management-related information only in approved systems of records associated with the applicable functional capability. Therefore, the PAR concept does not require any new records systems.

Although the PAR capabilities concept is not subordinate to or part of the current DoD Insider Threat Program, it aligns with and complements the Insider Threat Program by focusing on assessing and managing risks, at the installation and unit level of command, involving DoD personnel at risk for potentially violent behavior. As both efforts continue in the development process, the Department will take steps to synchronize the PAR capabilities with the DoD Insider Threat Program to forge a comprehensive Department effort that addresses and manages such risks.

Implementing the use of PAR capabilities closes out the actions stated by then-Secretary Gates in his August 18, 2010, memorandum directing the Department's responses to the Fort Hood Independent Review recommendations and by then-Secretary Hagel in his memorandum of March 26, 2013, directing actions based on the Defense Science Board (DSB) Task Force Report recommendations.



Attachments:

1. Purpose, Applicability, DoD PAR Policy, and Definitions
2. Responsibilities
3. PAR Content, Intent, and Standard Procedures
4. PAR Capabilities Training Standards and Education
5. Key Indicators of Potentially Violent Behavior

Attachment

1

ATTACHMENT 1

PURPOSE, APPLICABILITY, DOD PREVENTION, ASSISTANCE, AND RESPONSE (PAR) POLICY, AND DEFINITIONS

Purpose. Specifically, this memorandum:

- Provides commanders and equivalent civilian leaders with a risk-assessment mechanism (see Attachment 3 for further detail) to aid them in providing assistance and responses to their personnel at risk for potentially violent behavior.
- Directs the OSD Principal Staff Assistants to update appropriate DoD policies on workplace violence, insider threat, antiterrorism, and contract requirements related to contractor personnel to ensure that they are fully aligned.
- Directs the DoD Component heads to safeguard individual privacy and civil liberties in accordance with applicable law and policies in the implementation plans, processes, and procedures regarding the use of PAR capabilities.
- Explains the role of PAR functional experts in making their support functions available at the installation level by conducting information analysis and preparing input to commanders' and equivalent civilian leaders' risk assessments to aid these leaders in developing options to provide assistance to their personnel at risk for potentially violent behavior.
- Ensures that the PAR functional experts prepare their input in compliance with current records management policy prescribed in 44 U.S. Code Chapter 31, 36 C.F.R. Chapter XII, DoDI 5015.02, and applicable DoD Component records management regulations.
- Ensures that the PAR capabilities are carried out in compliance with the Privacy Act, DoD Directive 5400.11, DoD 5400.11-R, and applicable privacy program guidance.
- Prescribes standard PAR procedures for PAR functional experts to synchronize existing support functions and leverage other support functions to aid these functional experts in executing their mission.
- Prescribes requirements to train PAR functional experts and military and civilian personnel in the chain of command¹ in identifying and reporting indicators of potentially violent behavior.

¹ For purposes of this policy, chain of command includes supervisory chains when there is no applicable chain of command.

- Establishes a non-exhaustive list of numerous indicators of potentially violent behavior to support training DoD personnel on identifying and reporting potential violent behavior.

Applicability. This memorandum remains in effect until superseded by Departmental policy. This memorandum applies to:

- OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, and the Defense Agencies and DoD Field Activities who have jurisdiction over or operate DoD installations (referred to collectively in this memorandum as the “DoD Components”).
- National Guard personnel under Title 32 authority through the implementation of appropriate policy or regulations issued by the Secretaries of the Army and Air Force and the Chief, National Guard Bureau.
- Defense contractor personnel who have access to at least one DoD installation or facility, in accordance with the terms of their contracts.

This memorandum does not apply to:

- National Guard personnel in State active duty status.
- The reporting of criminal allegations or suspected criminal allegations involving DoD or DoD-affiliated persons to military criminal investigative organizations (MCIOs) or military department counterintelligence organizations (MDCOs) in accordance with DoD Instruction (DoDI) 5505.03 and DoDI 5240.04.

This memorandum does not affect DoD policy on continuous user activity monitoring on DoD information systems, a function that the DoD Chief Information Officer oversees in coordination with the Under Secretary of Defense for Intelligence (USD(I)) and in accordance with DoDI 8530.01; Counterintelligence Awareness and Reporting, a function that the USD(I) manages in accordance with DoDD 5240.06; or continuous evaluation background reviews on persons determined to be eligible for access to classified information, in accordance with Executive Order 13467 and the DoD Personnel Security Program in accordance with DoDI 5200.02.

DoD PAR Policy. It is DoD policy that:

- DoD Components will direct specific functional experts within existing support functions to coordinate with one another to provide, in accordance with privacy and records management laws, regulations, and policies (including 5 U.S.C. § 552a, DoDD 5400.11, DoD 5400.11-R, 44 U.S.C. Ch. 31, 36 C.F.R Ch. XII, and DoDI 5105.02), input to their commanders’ and equivalent civilian leaders’ risk assessments to aid these leaders in

developing options to provide assistance to their personnel at risk for potentially violent behavior. DoD Components may use existing procedures to satisfy the intent of this memorandum.

- DoD Components will use PAR capabilities in a way that satisfies the requirements prescribed in the March 26, 2013, Secretary of Defense memorandum.
- PAR functional experts will focus their capabilities on assisting commanders and their equivalent civilian leaders with providing help and assistance to all DoD personnel assigned to them (whether or not they have or had eligibility for a security clearance or sensitive position) who are at risk of potentially violent behavior.
- With respect to potentially violent behavior by DoD personnel who have been granted access to or are eligible for access to classified information, or that hold or are eligible to hold a sensitive position, PAR functional experts will refer indicators of that behavior to their Component Insider Threat Hub in accordance with Component policy.
- PAR functional experts will synchronize existing violence prevention programs and processes at the installation level to the extent possible, leverage other personnel support functions, and assist in the coordination between installation and unit commanders and their equivalent civilian leaders to identify and assess the risks of potentially violent behavior proactively.
- The PAR functional experts, in the performance of their official duties and when they have a need to know, consistent with privacy laws and policies, may query DoD Component Insider Threat Hubs to obtain additional information available under Federal law to aid them in providing input to their commanders' and equivalent civilian leaders' risk assessments on persons demonstrating indicators of potentially violent behavior.
- All DoD civilian and military personnel and supporting defense contractor personnel will receive training in accordance with the requirements in Attachment 3 of this memorandum in recognizing and reporting indicators of potentially violent behavior that could lead to violent acts or similar threat activities.
- Commanders and their equivalent civilian leaders will address potentially violent behavior as Force Protection (FP) issues because of the detrimental effects of violent behavior on the ability of the DoD Components to execute their missions. Responding to these effects requires commanders and their equivalent civilian leaders to apply many more capabilities than the traditional security precautions that are normally associated with FP.
- The indicators of potentially violent behavior listed in Attachment 5 serve as a ready reference and training aid for all DoD personnel, including commanders and their equivalent civilian leaders, to guide them in proactively reporting potentially violent behaviors that could lead to or indicate future violent acts to self or others.

- Disclosure of any PII with respect to indicators of potentially violent behavior listed in Attachment 5 to this memorandum must be consistent with DoD Directive 5400.11.
- Investigations initiated by an MCIO or MDCO have primacy over collateral investigations conducted by commanders, safety investigators, and other organizational entities and over PAR functional experts' information gathering and analysis. Collateral investigations and PAR functional experts' information gathering and analysis will not interfere or otherwise hinder criminal investigations.
- The MACB will monitor the implementation of this memorandum and assist in refining policy as appropriate.

DoD PAR Definitions. Unless otherwise indicated, the following definitions apply only to this PAR capabilities policy memorandum:

DoD Component Insider Threat Hub: A centralized multi-disciplinary staff element or activity, established by a DoD Component, that possesses an integrated capability to monitor, audit, fuse, and analyze incoming information for insider threat detection and mitigation. Hub personnel will be able to analyze information and activity indicative of an insider threat and refer that data to appropriate DoD officials to investigate or otherwise resolve.

Defense Insider Threat Management and Analysis Center (DITMAC): A cross-functional team of analysts that aggregates, integrates, reviews, analyzes, and shares information that is indicative of a potential insider threat. The DITMAC will exercise this information management capability (in concert with the DoD Components) with the ability to assess risk; refer issues for further consideration, investigation, and potential action; synchronize responses; and oversee resolution of identified issues across the Department within DoD-approved resources.

functional expert: A professionally trained and qualified individual representing a single discipline (examples of these disciplines are in paragraph 3.d. of Attachment 3) that contributes advice and information to their commanders' and equivalent civilian leaders' risk assessments to aid these leaders in developing options to provide assistance to their personnel at risk for potentially violent behavior.

MACB: The MACB, in accordance with DoDD 3020.40 and the Mission Assurance Strategy Implementation Framework, manages risk at the Department level through the MA Senior Steering Group (MA SSG) and the MA Executive Steering Group (MA ESG)).

PAR capabilities: A network of multi-disciplinary efforts, each led by a functional expert and normally resident on or available at the installation level, that commanders and their equivalent civilian leaders can use to aid them in identifying the level of risk that violent behavior poses to DoD personnel, organizations, installations, or separate facilities, and in developing risk-response recommendations to mitigate or remediate this risk. (See Attachment 3, paragraph 3.d. for a representative list of these capabilities.)

Risk assessment: Written (or oral, if appropriate) assessments that provide decision makers with information needed to understand factors that can negatively influence operation and outcomes, and make informed judgments concerning the extent of actions needed to reduce risk. They provide a basis for establishing appropriate policies and selecting cost-effective techniques to implement these policies. Risk assessments generally include the tasks of identifying threats and vulnerabilities and determining consequences.

Attachment

2

ATTACHMENT 2
RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR POLICY (USD(P)). The USD(P), in coordination with the Under Secretary of Defense for Personnel and Readiness (USD(P&R)), the USD(I), and the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), will:

a. Initiate, not later than 180 days from the date of this memorandum, updates to incorporate applicable portions of the policy in this memorandum in DoDI 2000.16, “DoD Antiterrorism (AT) Program,” and other appropriate DoD AT policies to comply with this memorandum.

b. Establish metrics to monitor the implementation of this memorandum via the MACB and ensure that the policies and procedures prescribed in this memorandum are incorporated in standing Departmental guidance.

c. Once the MACB has determined the DoD Components have fully implemented the requirements prescribed in this memorandum, coordinate with the USD(I), USD(P&R), and USD(AT&L) to initiate the process to cancel this memorandum or incorporate it into a DoD issuance as appropriate.

d. Ensure that there is a coherent collaboration process for issues of mutual interest regarding PAR and the DoD Insider Threat Program between the MACB and the Defense Security Enterprise Advisory Group (DSEAG).

e. Closely coordinate with the Assistant Secretary of Defense for Health Affairs (ASD(HA)) to review the results of the studies that the ASD(HA) is managing, evaluate recommendations from those studies, and refine policy as necessary.

f. As co-chair of the MACB, coordinate with the OSD Component heads to establish standards, guidelines, and sample procedures and to identify best practices. Evaluate the results of the studies on violent behavior required by the August 18, 2010, Secretary of Defense memorandum to refine applicable DoD policy and aid DoD Component heads in implementing this memorandum.

2. USD(P&R). The USD(P&R) will, within 180 days from the date of this memorandum:

a. Initiate updates, in coordination with the USD(AT&L), USD(P), and the USD(I), to all DoD policies addressing workplace violence (including DoDI 1438.06, “DoD Workplace Violence Prevention and Response Policy”) to ensure that these policies comply with this memorandum and cover all DoD military and civilian personnel and defense contractor personnel.

b. Coordinate with the USD(AT&L) to enable the USD(AT&L) to initiate updates to policies to require that defense contractors and their personnel comply with this memorandum.

c. Coordinate with the USD(AT&L) and the Assistant Secretary of Defense for Health Affairs (ASD(HA)) to provide the USD(P) and the MACB updates on the progress and results of studies on violent behavior required by the August 18, 2010, Secretary of Defense memorandum.

3. USD(I). The USD(I), in coordination with the USD(AT&L), USD(P), and USD(P&R), will:

a. Initiate, not later than 180 days from the date of this memorandum, updates to incorporate applicable portions of the policy within this memorandum in DoDD 5205.16, "The DoD Insider Threat Program," and other appropriate DoD insider threat policy and guidance.

b. Support the operating requirements of the PAR capabilities construct as appropriate.

c. Coordinate with the USD(P) to ensure there is a coherent collaboration process between the MACB and the DSEAG for issues of mutual interest regarding the PAR capabilities construct and the DoD Insider Threat Program.

4. USD(AT&L). The USD(AT&L), in coordination with the USD(P&R), will:

a. Incorporate the requirement for DoD workplace violence training for defense contractor personnel into the Defense Federal Acquisition Regulation Supplement or other appropriate policies.

b. Coordinate with the USD(P&R) to provide the USD(P) and the MACB updates on the progress and results of studies on violent behavior required by the August 18, 2010, Secretary of Defense memorandum.

5. DOD COMPONENT HEADS. The DoD Component heads, in consultation with servicing legal counsel, will:

a. Immediately establish procedures, consistent with applicable law and policy, to implement the use of PAR at the installation level, including joint bases, and in other organizations as the DoD Component heads direct, as prescribed in this memorandum and its attachments.

b. Develop procedures for assessing the risk of potentially violent behaviors; consider basing these procedures on accepted risk assessment guidance in Interagency Security Committee Standard: Violence in the Federal Workplace, Appendix A,² or the Association of Threat Assessment Professionals' Risk Assessment Guideline Elements for Violence:

² Available on the internet at:

https://www.dhs.gov/sites/default/files/publications/ISC%20Violence%20in%20the%20Federal%20Workplace_Appendix-A%20April%202013.pdf

Considerations for Assessing the Risk of Future Violent Behavior,³ or equivalent guidance; and ensure that the results of these procedures are credible, defensible, and reproducible.

c. Determine who within the existing support functions will serve as PAR functional experts, how these experts will network with one another to synchronize their risk management efforts, and how PAR functional experts will coordinate and engage with installation and organizational commanders and their equivalent civilian leaders to implement and monitor risk decisions.

d. Establish criteria specifying which indicators of potentially violent behaviors PAR functional experts must report to DoD Component insider threat hubs. At a minimum, the criteria will include the indicators listed in Attachment 5 to this memorandum and the approved DITMAC reporting thresholds.⁴ The criteria must also stipulate that information will be submitted to DoD Component insider threat hubs only when it applies to DoD-affiliated personnel who had or have been granted eligibility for access to classified information or eligibility to hold a sensitive position.

e. Establish procedures to train PAR functional experts on the requirements in this memorandum.

f. Establish procedures to train their DoD civilian employees, military personnel, and defense contractor personnel on:

(1) Identifying and reporting the indicators of potentially violent behaviors listed in Attachment 5 to this memorandum.

(2) The role of PAR functional experts in performing information analysis and providing input to their commanders' and equivalent civilian leaders' risk assessments.

(3) The role of law enforcement organizations in cases of emergencies involving violent behavior.

g. Ensure that all commanders, managers, and supervisors understand how PAR functional experts synchronize and leverage existing violence prevention programs and processes to aid them in responding to instances of potentially violent behavior.

h. Ensure that PAR functional experts make their capabilities available to installation, organizational, and off-installation facility commanders and their equivalent civilian leaders.

i. Establish procedures to enable PAR functional experts to interface with local authorities, as appropriate, to aid PAR functional experts in assessing the risk from violent behavior.

³ Available on the internet at: <https://sm.asisonline.org/ASIS%20SM%20Documents/RageV0407.pdf>

⁴ Available from the Office of the USD(I).

j. Keep the USD(P) informed, through the MACB, of the progress made and resources required for implementing the requirements in this memorandum.

k. Coordinate with the Deputy Chief Management Officer (DCMO) to establish procedures for reporting and managing incidents involving potentially violent behavior for their personnel operating within the Pentagon Reservation and designated DoD facilities in the National Capital Region (NCR), including whether the DCMO or the DoD Component head has primary responsibility for those personnel.

l. Establish procedures to report indicators or patterns of potentially violent behaviors consistent with the indicators in Attachment 5 to this memorandum through the chain of command to their respective policy and security management organizations.

6. OSD COMPONENT HEADS. The OSD Component heads will coordinate with the DCMO to prescribe procedures for their organizations operating on the Pentagon reservation and designated DoD facilities in the NCR to report violent behavior and similar threat information.

7. DCMO. The DCMO will:

a. In addition to the DCMO's responsibilities as Senior Official for the OSD Insider Threat Program and in coordination with the DoD Component heads having personnel operating within the Pentagon Reservation and designated DoD facilities in the NCR, establish procedures for implementing this memorandum.

b. Coordinate with the DoD Component heads operating on, or with subordinate organizations operating on the Pentagon reservation and designated DoD facilities in the NCR, to establish threat-management capabilities to address potentially violent behaviors.

c. Establish, in coordination with the OSD Principal Staff Assistants and other appropriate DoD Component heads, communications channels to share appropriate information on potentially violent behaviors.

Attachment

3

ATTACHMENT 3

PAR CONCEPT, INTENT, AND STANDARD PROCEDURES

1. The PAR Capabilities Concept and Intent. The PAR capabilities concept is a proactive effort to network and synchronize existing support functions to enable PAR functional experts to gather, share, and analyze more information on incidents of potentially violent behavior than they could operating independently. The PAR capabilities concept enables functional experts to provide input and risk response recommendations to commanders and their equivalent civilian leaders for their risk assessments and risk decisions. The purpose of the PAR capabilities concept is to aid these leaders in helping persons at risk for potentially violent behavior before these persons commit violent acts to themselves or other DoD personnel.

a. Procedures for Reporting Indicators of Potential Violent Behavior.

(1) Personnel who witness behavior in another person that is detrimental to organizational operations, is well outside normal behavior, causes reasonable concern in others, and is consistent with any of the indicators in Attachment 5 of this memorandum will report the indicators in accordance with their DoD Component reporting procedures.

(2) The chain of command will refer the matter to the appropriate PAR functional experts.

(3) If a PAR functional expert receives the information concerning the indicators before the chain of command does, the PAR functional expert will inform the chain of command, pursuant to all appropriate ethical, privacy, and civil liberties criteria.

b. Procedures for Information Sharing.

(1) PAR functional experts may exchange information concerning the indicators of potentially violent behavior with other PAR functional experts, and with appropriate organizations internal and external to DoD, to the extent such exchange is consistent with the classification of the information and the DoD Information Security Program (see Volumes 1-4 of DoD Manual 5200.01), the Privacy Act and the DoD privacy program (see DoDD 5400.11 and DoD 5400.11-R), and applicable Component records management procedures. Personally identifiable information (PII) must be protected, consistent with DoDD 5400.11 and DoD 5400.11-R.

(2) PAR functional experts may query their own DoD Component Insider Threat Hub for additional information to aid them in developing input to their commanders' and equivalent civilian leaders' risk assessments on indicators of potentially violent behavior involving cleared personnel. If any PAR functional expert needs to query other DoD Components' Insider Threat Hubs for additional information on cleared personnel, the PAR functional expert will first obtain permission from his or her own DoD Component Insider Threat Hub.

(3) PAR functional experts will develop input to their commanders' and equivalent civilian leaders' risk assessments, independently of the other PAR functional experts, and then share only their respective input with one another to ensure that the final input to their commanders' and equivalent civilian leaders' is synchronized and as complete as possible (see paragraph 1.c. of this Attachment for further detail). DoD Component heads will ensure that such collection, maintenance, and sharing of information complies with the Privacy Act.

(4) PAR functional experts will share information from their records systems with other PAR functional experts only if the information is relevant to a reported indicator of potentially violent behavior and only if their commanders would normally be authorized access to that information.

(5) PAR functional experts will not submit information directly to the DITMAC.

c. PAR Capabilities Functional Experts' Mission. Each capability within the PAR capabilities construct (see paragraph 3.d of this Attachment) will be led by a functional expert, normally located at the military installation level. PAR functional experts coordinate with one another to synchronize existing violence prevention capabilities and process efforts and conduct risk management related to potentially violent behaviors that could lead to violent acts and similar threat activities. PAR functional experts:

(1) Serve as a means by which commanders and their equivalent civilian leaders coordinate with their DoD Component Insider Threat Hub for exchanging information on DoD or DoD-affiliated personnel who had or have been granted eligibility for access to classified information or eligibility to hold a sensitive position. This function enables these leaders to have access to information that the DoD insider threat enterprise has passed to the DoD Component Insider Threat Hubs, and aids them in increasing their understanding of situations involving individuals at risk for potentially violent behavior.

(2) Provide commanders and their equivalent civilian leaders with input to support these leaders' risk assessments for incidents of potentially violent behavior that may involve DoD personnel or defense contractor personnel.

(3) In preparing the input to the risk assessments, PAR functional experts will consider the likelihood of violent behavior occurring; its impact on the organization's mission; the nature, sources, and causes of the potential violent behavior; and the level of risk the potentially violent behavior poses to the organization. Such input must be maintained in compliance with the Privacy Act.

(4) Synchronize, at the installation level and consistent with applicable law, existing personnel management, mental health, law enforcement, criminal investigation, and security functions to focus on identifying and assessing risks from potentially violent behavior and on recommending response actions to reduce these risks.

(5) Ensure that all relevant information from these functions is made available to commanders and their equivalent civilian leaders to inform risk decisions within the limitations of applicable law and policies, including the policies listed in Attachment 4.

(6) Consider referrals to assistance programs in their risk response recommendations to commanders and their equivalent civilian leaders to help personnel at risk for potentially violent behavior.

(7) Maintain records containing information used in the development of risk assessments and decisions in accordance with 36 C.F.R. Ch. XII, DoDI 5015.02, applicable DoD Component records management regulations, and the DoD Component's Records Disposition Schedule. In addition, maintain such records, in authorized systems of records in compliance with the Privacy Act (5 U.S.C. § 552a), DoDD 5400.11 and DoD 5400.11-R.

d. Chain of Command Mission. Commanders and their equivalent civilian leaders in the chain of command to which the person at risk for potentially violent behavior is assigned review the PAR functional experts' risk-response recommendations in accordance with their Component policies, regulations, and guidance; coordinate as necessary with the installation chain of command; and issue risk decisions designed to assist the person at risk for potentially violent behavior and to reduce the risks to the extent possible to their installation, organization, personnel, and mission.

2. PAR Capabilities Standard Procedures. The PAR functional experts:

a. Contact law enforcement immediately if any of the functional experts believe the indicators warrant emergency or other time-sensitive response, or are indicative of criminal allegations or suspected criminal allegations involving DoD personnel or persons affiliated with the DoD or any property or programs under the Department's control or authority.

b. Consult the organization's security manager to determine whether or not the subject of the report of indicators of potentially violent behaviors has or had been granted eligibility for access to classified information or eligibility to hold a sensitive position. If so, the functional experts, as a group, contact the DoD Component insider threat hub to enable it to assess the risk of the incident pursuant to DoD Insider Threat program procedures. PAR functional experts will continue to assess the risk in instances where the person at risk has never been granted eligibility for access to classified information or eligibility to hold a sensitive position.

c. Determine, as a group, and in consultation with the commander or equivalent civilian leader, whether or not it is necessary to convene to provide input to these leaders' risk assessments on the reported indicators.

d. Gather sufficient information to produce the input to their commander's or equivalent civilian leader's risk assessment. Maintain this information and input in an appropriate system of records in accordance with DoD privacy and records management policies.

e. Prepare risk-response recommendations on the reported indicators to inform unit and installation commanders' and their equivalent civilian leaders' risk decisions.

f. Monitor the commander's and their equivalent civilian leaders' risk decisions and develop recommendations, as appropriate, for these leaders to improve the effectiveness of those risk decisions.

3. DoD Component heads will:

a. Establish procedures to implement, based on existing resources, the requirements in this memorandum.

b. Establish procedures for individuals to report indicators of potentially violent behavior in a safe environment that is free from harassment, retaliatory actions, and unlawful discrimination.

c. Ensure that PAR functional experts use official, appropriately secure communication channels, such as encrypted e-mail, to report and receive information on incidents of potentially violent behaviors or similar threat activities, and that unauthorized data repositories of these incidents are not created or used, consistent with the Privacy Act and DoD privacy policies.

d. Ensure that unit and installation commanders and their equivalent civilian leaders have the following functional resources available and know how to access them. Each function listed is a PAR capability. These personnel must be professionally trained and qualified per Departmental or Component standards. Commanders and their equivalent civilian leaders can tailor these capabilities as the violent behavior or similar threat incidents dictate:

- (1) Legal.
- (2) Military personnel management.
- (3) Civilian personnel management.
- (4) Defense contract administration.
- (5) Chaplain.
- (6) Military Criminal Investigative Organization (MCIO).
- (7) Family advocacy, suicide prevention, sexual assault, and drug and alcohol programs.
- (8) Mental health.
- (9) Law enforcement and physical security.
- (10) Personnel security
- (11) Industrial security.
- (12) Information security and assurance, including digital information protection.
- (13) Privacy program.

e. Prescribe procedures for installation commanders and their equivalent civilian leaders to engage with off-installation authorities, such as the Department of Veterans Affairs and law enforcement officials, as needed to execute their responsibilities assigned in this memorandum.

4. Commanders and equivalent civilian leaders of organizations other than DoD installations will:

a. Establish efficient means for DoD military and civilian personnel and defense contractor personnel to report indicators of potentially violent behaviors to a PAR functional expert or the chain of command.

b. Ensure that these personnel have access to the indicators of potentially violent behaviors and the approved DITMAC reporting thresholds.

c. Establish procedures to train these personnel to recognize and report through the proper channels the indicators of potentially violent behaviors listed in Attachment 4 of this memorandum.

5. Commanders and equivalent civilian leaders of DoD installations. Commanders and equivalent civilian leaders of installations, in addition to the responsibilities listed in paragraph 4 of this attachment, will:

a. Identify and assign personnel within existing support functions to serve as PAR functional experts.

b. Establish procedures to exchange risk-response recommendations with commanders and equivalent civilian leaders of organizations assigned to and tenants on the installation, as well as commanders and equivalent civilian leaders of off-installation facilities under their security responsibility.

Attachment

4

ATTACHMENT 4

PAR CAPABILITIES TRAINING STANDARDS AND EDUCATION

1. Training standards for PAR functional experts. Training will include:

a. Familiarization with and reporting procedures for CI insider threat anomalies listed in DoDD 5240.06, “Counterintelligence awareness and reporting (CIAR),” and DoDI 5240.26, “Countering Espionage, International Terrorism, and Counterintelligence (CI) Insider Threat.”

b. Procedures on how the various functional experts can respond to instances of active violent behavior and potentially violent behavior or similar threat activities.

c. Applicable laws and regulations on collecting, integrating, retaining, safeguarding, and using records and information, and the consequences of misuse of this information. At a minimum, the following should be included:

(1) The Privacy Act (5 U.S.C. § 552a) and the DoD privacy program (including DoDD 5400.11 and DoD 5400.11-R).

(2) DoD health information privacy in accordance with DoDI 6490.08 and DoD 6025.18-R.

(3) DoD civil liberties in accordance with DoDI 1000.29.

(4) Suspicious activity reporting in accordance with DoDI 2000.26.

(5) How DoD law enforcement collects, maintains, uses, and disseminates PII in accordance with DoDI 5505.17.

(6) DoD records management in accordance with DoDI 5015.02.

d. Procedures to provide input to their commanders’ and equivalent civilian leaders’ risk assessments and to aid these leaders in developing options to provide assistance to their personnel at risk for potentially violent behavior.

e. Referral procedures in accordance with Section 811 of the Intelligence Authorization Act of 1995 (Public Law 103-359), or to the Inspector General or MCIOs.

f. Referral procedures to other health care, personnel management, and support programs, including:

(1) Suicide prevention.

(2) Family advocacy.

(3) Alcohol and drug abuse prevention and treatment.

- (4) Mental health, or other health care as necessary.
- (5) Combat and operational stress control.
- (6) Counseling services for DoD personnel and their family members.
- (7) Occupational health.
- (8) Personnel management.
- (9) Sexual assault response coordinator.

2. Training requirements for all personnel. DoD Component heads will establish procedures, including appropriate refresher training, to ensure that all assigned DoD personnel and defense contractor personnel, especially commanders, supervisors, law enforcement, and security personnel, receive training on the following topics in this section within 30 days of entry on duty (or a similarly prompt timeframe for Reserve Component personnel), granting of a security clearance, or start of performance on a contract:

- a. The organization's workplace violence prevention policy, including the obligations and privileges that DoD personnel have pursuant to it.
- b. Recognizing and reporting indicators of potentially violent behaviors, as listed in Attachment 5 to this memorandum.
- c. The role of PAR functional experts in performing information analysis to develop input to their commanders' and equivalent civilian leaders' risk assessments.
- d. The role of law enforcement as a first responder, especially during emergencies where violent behavior threatens DoD personnel with injury or death.
- e. Current and potential means of violent behavior, including mishandling, damage, and theft of DoD information, assets, and resources. This topic is vital to the Department to keep DoD personnel advised on current trends in violent behavior.

Attachment

5

ATTACHMENT 5

KEY INDICATORS OF POTENTIALLY VIOLENT BEHAVIOR

1. These indicators of potentially violent behavior serve as a ready reference and training aid for DoD personnel, including commanders and their equivalent civilian leaders, to guide them in proactively reporting potentially violent behaviors that could lead to or indicate future violent acts to self or others. The indicators also aid PAR functional experts in determining what assistance they can provide to persons at risk for potentially violent behavior.
2. Preventing violent behavior is significantly enhanced when DoD personnel observe potential indicators and know that their concerns, once reported, will be handled appropriately. Although none of these indicators should be ignored, it is important to understand that they should be documented when they do occur, such as during performance reviews pursuant to DoDI 1400.25, volumes 1404 and 2011, and similar performance counseling policy, to aid in identifying behavior that is well outside normal behavior. The list of behaviors and actions below is not exhaustive and is not a checklist, but the list provides possible behaviors and activities that should be reported through all appropriate and mandatory channels if an individual is exhibiting actions that cause reasonable concern to other persons.
3. These indicators were derived from multiple sources, including the Interagency Security Committee and the Federal Bureau of Investigation' Behavioral Science Unit. The Defense Health Agency is also managing ongoing studies to aid in identifying potential violent behavior. When complete and published, the results of these studies will be used to improve this construct. Although no single behavior or action can predict violent behavior or insider activity with certainty, when such events occur, witnesses and victims often report they noticed changes in the individual's behavior, mood, or performance prior to the event.
4. In addition to being familiar with the indicators in this attachment (listed below), commanders, their equivalent civilian leaders, and all managers and supervisors should also be mindful of DoD personnel who have experienced, or who are experiencing, various organizational or personal events (e.g., loss of employment or loss of a personal relationship) that may signal a need for help or assistance. These changes can take many forms, but often include one or more of the following indicators:
 - Direct, indirect, or veiled threats of harm or violence
 - Intimidating, belligerent, harassing, bullying, or aggressive behavior
 - Numerous conflicts with supervisors and other employees
 - Bringing an unauthorized weapon to the workplace, brandishing a weapon in the workplace, making inappropriate references to the use of guns, or unusual fascination with weapons (**see note**)
 - Statements indicating the individual is involved in criminal activity
 - Statements showing fascination with incidents of workplace violence, statements indicating approval of the use of violence to resolve a personal or professional problem, or statements indicating identification with perpetrators of workplace homicides
 - Statements indicating desperation (over family, financial, and other personal problems) to the point of contemplating suicide

- Drug/alcohol abuse
- Extreme changes in behavior, personality, or performance
- Acquisition of multiple weapons (**see note**)
- Significant escalation in off-duty, non-work-related target practice or weapons training (**see note**)
- Menacing actions with weapons
- Undue interest in explosives
- Undue interest in previous shootings or mass attacks
- Conveying a direct or veiled threat of violence to a third party
- Committing physical assault or wrongful physical violence
- Engaging in conduct that warrants physical restraint or confinement
- Stalking or surveilling an individual or individuals
- Wrongfully damaging or destroying property
- Blatant or intentional disregard for the safety of others
- Disruptive, aggressive, or angry language
- Unusually poor work performance or disciplinary problems at the work site
- Commission of a violent misdemeanor or felony at the work site
- Delusional statements or paranoid ideas
- Increased isolation
- Unusual depressed mood
- Suicidal ideations

NOTE: In accordance with subsection 1062(a) of the Ike Skelton National Defense Authorization Act for Fiscal Year 2011, as amended, DoD may not collect or record any information relating to the otherwise lawful acquisition, possession, ownership, carrying, or other use of a privately owned firearm, privately owned ammunition, or another privately owned weapon by a member of the Armed Forces or a DoD civilian employee on property that is not (1) a military installation; or (2) any other property that is owned or operated by the Department of Defense. Pursuant to subsection 1062(c), this limit does not apply to:

- (1) creating or maintaining records relating to, or regulating the possession, carrying, or other use of a firearm, ammunition, or other weapon by a member of the Armed Forces or DoD civilian employee while (A) engaged in official DoD duties; or (B) wearing the uniform of an Armed Force;
- (2) creating or maintaining records relating to an investigation, prosecution, or adjudication of an alleged violation of law (including regulations not prohibited under subsection (a)), including matters related to whether a member of the Armed Forces constitutes a threat to the member or others [Note that this provision doesn't apply to DoD civilian employees]; or
- (3) authorizing a health professional that is a member of the Armed Forces or a DoD civilian employee or a commanding officer to inquire if a member of the Armed Forces plans to acquire, or already possesses or owns, a privately-owned firearm, ammunition, or other weapon, if such health professional or such commanding officer has reasonable grounds to believe such member is at risk for suicide or causing harm to others.

TAB

B

SERVICE APPROACHES TO
INSIDER THREAT AND WORKPLACE VIOLENCE

- USD(I) has established the Insider Threat program. Its status is as follows:
 - The DITMAC has attained “Provisional Initial Operating Capability”, meaning that the DITMAC has acquired and occupied its workspace in Crystal City, hired staff, drafted a DoD Instruction to frame its operational responsibilities, and built the capability to receive information.
 - The DITMAC lacks the authority to analyze and share insider threat information containing Personal Identifying Information, as its Systems of Records Notice (SORN) has not been approved.
- Since the 2009 Fort Hood shootings, the Components have undertaken a range of approaches to address insider threat. For example:
 - U.S. Navy: The Navy established its insider threat program in OPNAV Instruction 5510.165A and is implementing a process to aggregate and analyze User Activity Monitoring (UAM), Continuous Evaluation (CE), human resources (HR), law enforcement (LE), counterintelligence (CI), medical, inspector general, physical security, and other authorized data sources in order to deter, detect, respond to, and mitigate risks of insider threat activities across the Navy.
 - US Marine Corps: The Deputy Commandant, Plans, Policies, and Operations at Headquarters, Marine Corps serves as the Marine Corps Protection Advocate and is responsible for the Marine Corps Insider Threat Program. The Marine Corps Insider Threat Working Group (MCITWG) was established in October 2010, and the USMC Analysis Center was created in September 2015. Many elements of the Marine Corps program such as the Violence Prevention Program and unit Force Preservation Councils have existed for many years and are integrated into the overall Insider Threat Program. The focus of the Marine Corps Insider Threat Program is prevention through application of Marine Corps leadership principles and reporting of "issues of concern" through existing means. Communication between the Analysis Center and Commanding Officers is critical for full and effective implementation of the program. The Marine Corps Insider Threat Analysis Center is supported by the Marine Corps Intelligence Activity (MCIA) which focuses on UAM for the Joint Worldwide Intelligence Communications System (JWICS)."
 - U.S. Army: The Army established its insider threat program with the Deputy Chief of Staff for Operations (G-3/5/7) and the Assistant Secretary of the Army (Manpower & Reserve Affairs) designated as co-Senior Officials. The Army Protection Directorate (G-34) has the responsibility to synchronize the program across multiple lines of effort within the Army. The Army is currently conducting UAM on the JWICS network with plans to expand UAM on the Secret Internet Protocol Router Network (SIPRNET) beginning in FY2017. The Army continues to implement a phased Initial Operating

Capability for the Army Insider Threat Hub while working towards Full Operational Capability in FY2019.

- U.S. Air Force: The Air Force established its insider threat program in Air Force Instruction 16-1402. It specifies an integrated framework of policies and procedures to detect, deter, and mitigate insider threats; develop training on existing and emerging insider threats; implement continuous evaluation of personnel through enhanced monitoring of user activity on information systems; leverage antiterrorism (AT), counterintelligence (CI), human resources (HR), law enforcement (LE), security, medical, and other authorities to improve existing insider threat detection and mitigation efforts; and ensure that civil liberties and privacy rights are safeguarded.

TAB

C

Turner, Larry N CTR OSD OUSD POLICY (US)

From: Jacobson, Kyle R CIV OSD OGC (US)
Sent: Friday, January 13, 2017 1:56 PM
To: Breuker, Theodore A Col USAF OSD OUSD POLICY (US); Turner, Larry N CTR OSD OUSD POLICY (US)
Cc: Kusiak, Pauline M CIV OSD OUSD POLICY (US); Ablin, Erik J CIV OSD OGC (US); Devendorf, Kristi A CIV OSD OGC (US)
Subject: Close Out of Actions Directed in Response to Fort Hood Recommendations: Capabilities for Managing the Risk from Violent Behavior and Similar Threats
Attachments: TAB A - PAR Policy Memo v16 (Principal Coord) (OGC edits Jan 12)(ea).docx; Action Memo 15 Dec 16 vers (Principal Coord) (OGC edits 12-30-16).docx
Signed By: kyle.r.jacobson.civ@mail.mil

Ted and Larry,

OGC coordination is by Mr. Robert S. Taylor, Principal Deputy General Counsel, as revised. The revisions are reflected in tracked changes in the attached files.

Please let me know if you have any questions.

v/r
Kyle

KYLE R. JACOBSON
Associate Deputy General Counsel, International Affairs Office of the General Counsel of the Department of Defense
(571) 256-8380 (DSN 260-8380)

CAUTION: Information contained in this message may be protected by the attorney/client, attorney work product, deliberative process or other privileges. Do not disseminate further without approval from the Office of the DoD General Counsel.

TAB

D

UNCLASSIFIED

Policy Coordination Sheet

Subject: Close Out of Actions Directed in Response to Fort Hood Recommendations:
Capabilities for Managing the Risk From Violent Behavior and Similar Threats

Control Number: USP003114-16

| Title/Organization | Name | Coordination Requested | Coordination Received |
|---------------------------|------------------------------|-------------------------------|------------------------------|
| DCMO | David Tillotson III | Oct 28, 2016 | Jan 12, 2017 |
| USD(P&R) | Peter Levine | Oct 28, 2016 | Nov 8, 2016 |
| CIO | Terry Halvorsen | Oct 28, 2016 | Nov 28, 2016 |
| ASD(LA) | Louis Lauter | Oct 28, 2016 | Nov 10, 2016 |
| CAPE | Jamie M. Morin | Oct 28, 2016 | Nov 18, 2016 |
| ATSD(PA) | Jeremy Martin | Oct 28, 2016 | Nov 18, 2016 |
| USD(AT&L) | Alan Estevez | Oct 28, 2016 | Dec 9, 2016 |
| USD(I) | Todd R. Lowery | Oct 28, 2016 | Jan 18, 2017 |
| USD(C) | John Conger | Oct 28, 2016 | Nov 22, 2016 |
| Army | Eric K. Fanning | Oct 28, 2016 | Jan 10, 2017 |
| Navy | Janine A. Davidson | Oct 28, 2016 | Jan 10, 2017 |
| Air Force | Deborah L. James | Oct 28, 2016 | Jan 5, 2017 |
| National Guard Bureau | MG James Witham | Oct 28, 2016 | Nov 18, 2016 |
| CJCS | Maj Gen Jacqueline Van Ovost | Oct 28, 2016 | Dec 1, 2016 |
| OGC | Robert S. Taylor | Oct 28, 2016 | Jan 13, 2017 |
| DC&MA | Pauline Kusiak | Jan 13, 2017 | Jan 13, 2017 |

UNCLASSIFIED