RESEARCH NOTE

Abstract

As part of a recent assessment of DoD's workplace violence prevention programs, researchers reviewed the implementation status of the mandatory Prevention, Assistance, and Response (PAR) capabilities. The review found a number of barriers to implementation, many due to the fact that the PAR concept emerged from a complex array of insider threat events and policies related to workplace violence prevention, counter-insider threat, and personnel vetting. The purpose of this Research Note is to analyze this history to help policymakers move forward with efforts to integrate various stakeholders' needs into a comprehensive strategy to protect the DoD workforce.

the ThreatLab
Integrating Research Into Practice

About The Threat Lab

The Defense Personnel and Security Research Center (PERSEREC) established The Threat Lab in 2018 to realize the DoD Counter-Insider Threat Program Director's vision to integrate the social and behavioral sciences into the mission space. To subscribe to The Threat Lab's distribution list, please email dodhra.ThreatLab@mail.mil

The PAR Capabilities and the Convergence of Workplace Violence Prevention, Counter-Insider Threat, and Personnel Vetting Policies in DoD

James Beneda & Stephanie L. Jaros

Introduction

Researchers from *The Threat Lab* recently conducted a comprehensive policy and implementation status review of the Prevention, Assistance, and Response (PAR) capabilities as part of a larger project on DoD's violence prevention efforts. The February 2, 2017 Deputy Secretary of Defense Memorandum (hereinafter, PAR Memo) established the PAR capabilities, and served to close out DoD's 2010 Independent Review of the November 2009 shootings at Fort Hood, Texas. The PAR Memo defined the PAR capabilities as:

> 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.[1] (p. 4)

As the project got underway, researchers quickly discovered a number of barriers to the effective implementation of the PAR capabilities. For example, basic terms were not clearly defined (*e.g.*, installation, commanders, personnel, risk), and follow-up interviews revealed that stakeholders disagreed about the scope of the PAR capabilities and the intent of the PAR concept itself.

A closer analysis of the PAR requirements suggested that the PAR Memo's authors operated from a number of unstated assumptions about how the capabilities would function and what they should

[1] Deputy Secretary of Defense. (February 2, 2017). *Final implementation action of Fort Hood recommendations: Managing potentially violent behavior through prevention, assistance, and response capabilities* [Memorandum].

achieve. This was particularly evident in discussions with subject matter experts about the PAR Memo's guidance on how PAR "aligns with and complements" DoD- and Component-level Insider Threat Programs.

To better understand these unstated assumptions and the organizational context from which the PAR Memo emerged, researchers expanded the project and analyzed a series of policy decisions and insider threat events that occurred both before and after the PAR Memo's official release. As illustrated in Figure 1 below, the expanded review found that DoD issued the PAR Memo in a rapidly changing environment in which disparate divisions across the Office of the Secretary of Defense responsible for workplace violence prevention, counter-insider threat, and personnel vetting policies were converging independently around a common need for effective risk assessment and mitigation capabilities.

The purpose of this Research Note is to demonstrate how the PAR Memo was both a response to and a symptom of insufficiently synchronized efforts across multiple mission spaces. The results of this review are intended to inform policymakers and, in so doing, help move efforts forward to integrate all relevant stakeholders' needs into a comprehensive strategy to protect the DoD workforce.

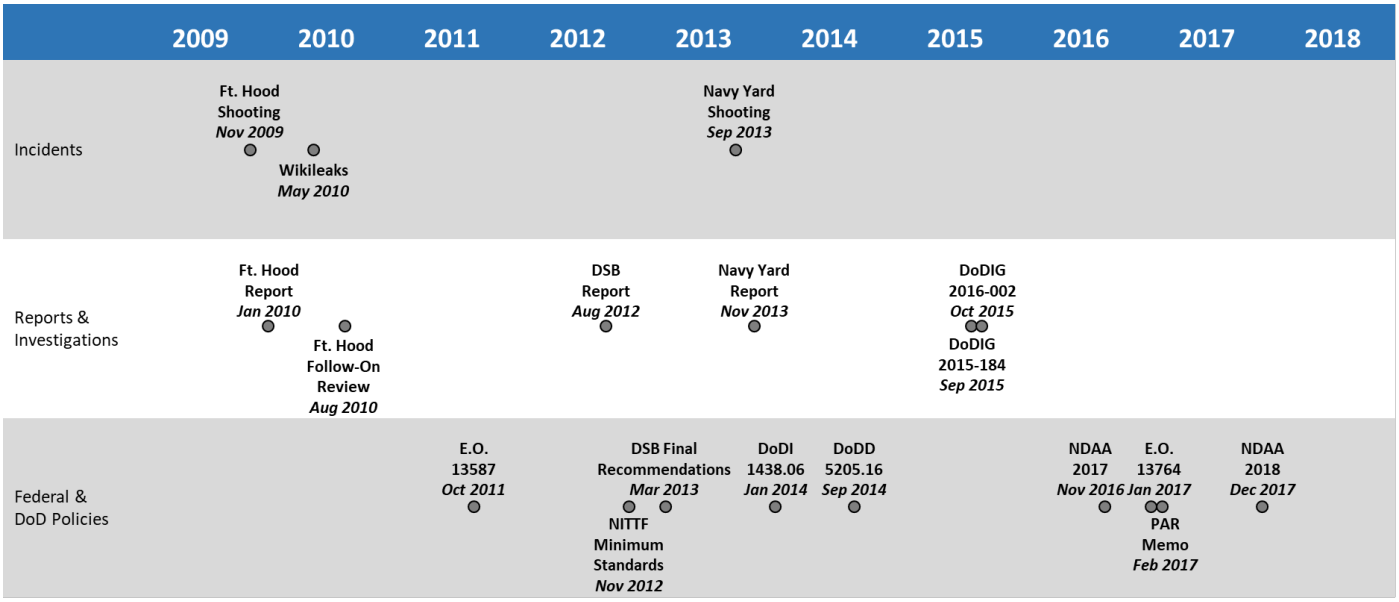

Figure 1. Timeline of Incidents, Reports and Investigations, and Policy Issuances

Policy Origins of PAR

Internal Reviews of the Fort Hood Shooting

DoD's January 2010 Independent Review of the 2009 Fort Hood shooting laid the foundation for the PAR concept.[2] First, it found that DoD lacked comprehensive guidance on workplace violence prevention and response. Second, it recommended that DoD develop threat management unit (TMU) capabilities, modeled on those of the Navy and present in other organizations, to provide commanders with a cadre of multidisciplinary experts to:

[2] Department of Defense Independent Review Related to Fort Hood. (2010). *Protecting the force: Lessons from Fort Hood*. Washington, DC: Department of Defense.

- Assess the risk of potential violence among DoD personnel;
- Readily share personnel, law enforcement, and medical records of at-risk individuals among TMU members and commanders; and
- Integrate existing programs such as suicide, sexual assault, and family violence prevention within a comprehensive violence prevention and response program.

The August 2010 follow-on review of the Fort Hood shooting, directed by then-Secretary of Defense Robert Gates, laid out specific policy actions for implementing the Independent Review's 79 recommendations.[3] Briefly, it emphasized the need to broaden the scope of DoD's traditional force protection models to include internal threats. To achieve this, the 2010 follow-on review placed ultimate responsibility for violence prevention on DoD leaders at all levels. Secretary Gates wrote that force protection was "not a substitute for leadership" and reminded leaders of their duty "to take appropriate action to prevent and respond to potential problems, whatever their cause" (pp. 1-2).

The August 2010 follow-on review also directed the Defense Science Board (DSB) to undertake a formal study on predicting and managing internal threats of targeted violence.[4] The DSB study, published in 2012, concluded there was "no effective formula for predicting violent behavior with any degree of accuracy," and that "prevention should be the goal rather than prediction" (p. 2). This was best achieved by encouraging workers to report potentially harmful behaviors they observed to commanders and multidisciplinary professionals who could then proactively intervene to assess and mitigate any risks. Like the 2010 Fort Hood Independent Review, the 2012 DSB study recommended DoD adopt a TMU model to promote early detection, facilitate information sharing, and leverage expertise from multiple disciplines such as law enforcement, risk assessment, mental health, and the social and behavioral sciences. However, the 2012 DSB study also identified a number of challenges to implementing a TMU model, including cultural stigmas around self and peer reporting, and the need to shift DoD's operational focus from a traditional disciplinary response to a new paradigm of support and assistance.

The Navy Yard Internal Review

In March 2013, a memorandum issued by then-Secretary of Defense Chuck Hagel formally directed adoption of a TMU model by DoD and its Components.[5] The plan required DoD to set minimum policy requirements no later than October 2013 for Components to begin implementing TMU capabilities. However, DoD-level policy guidance was delayed for several years and never fully realized. This delay was due in large part to another high-profile incident of targeted violence on September 16, 2013 at the Washington Navy Yard.

While the 2009 Fort Hood shooting revealed the broad range of DoD's strategic vulnerabilities to targeted violence, the 2013 Navy Yard shooting highlighted systemic failures to access, integrate, and synchronize critical information that could be used to identify, assess, and mitigate risks of targeted

[3] Secretary of Defense. (August 18, 2010). *Final recommendations of the Ft. Hood follow-on review* [Memorandum]. Washington, DC: Department of Defense.
[4] Defense Science Board. (2012). *Task force report: Predicting violent behavior*. Washington, DC: Department of Defense.
[5] Secretary of Defense. (March 26, 2013). *Final recommendations of the Defense Science Board report on predicting violent behavior* [Memorandum]. Washington, DC: Department of Defense.

violence and other insider threats.[6] The 2013 Navy Yard Internal Review found DoD lacked the capability to assess risks in a "whole person" context due to "the lack of a single centralized function or authority with the responsibility to aggregate, evaluate, and appropriately disseminate insider threat information" (p. 22). The 2013 Navy Yard Internal Review found that "neither the personnel security process nor the physical security capability is equipped or designed to prevent" (p. 4) such incidents and concluded, in agreement with both the 2010 Fort Hood Independent Review and 2012 DSB study, that the only truly effective approach to threat prevention is early detection and intervention.

The 2013 Navy Yard Internal Review emphasized and recommended the expansion of centrally managed continuous evaluation (CE) programs that could generate actionable threat warnings from across the DoD workforce. The suggestion that CE should be applied to ongoing employee suitability and fitness issues in addition to national security eligibility acknowledged the fact that a large portion of the DoD workforce (*i.e.*, non-cleared civilian and contractor employees) fell outside the scope of existing workplace violence and insider threat prevention policies.

The 2013 Navy Yard Internal Review asserted that neither effective insider threat management capabilities nor meaningful physical security reforms could be achieved without a comprehensive CE program. Achieving this, however, would require a shift in the CE concept, which was, at the time, usually understood as a system of automated records checks intended to supplement personnel security vetting.[7] In contrast, the 2013 Navy Yard Internal Review defined CE as a strategic capability for generating "informed decisions regarding the trustworthiness of DoD personnel based on the composite of organizational information and the linkage of that information through technology infrastructure" (p. 22). Further, it argued that if done well, a comprehensive CE strategy would change attitudes toward peer and supervisor reporting and lead the workforce to view early intervention as a more reliable, less adversarial, and less punitive means of threat prevention.

DoDIG Workplace Violence Assessment

Two years later in 2015 the DoD Office of the Inspector General (DoDIG)[8] evaluated DoD's workplace violence prevention efforts and found that, despite 5 years of policy responses following Fort Hood, DoD still lacked a comprehensive workplace violence prevention and response program. DoDIG also found that DoD Components applied policy inconsistently across military, civilian, and contractor personnel. For instance, DoD's formal workplace violence policy, issued in 2014, applied only to the civilian workforce.[9] Although the policy required Components to establish and properly train multidisciplinary threat assessment teams, it provided no implementation guidance and did not integrate the program into any existing threat management capabilities. An official from the Office of

---

[6] Under Secretary of Defense for Intelligence. (November 20, 2013). *Internal review of the Washington Navy Yard shooting: A report to the Secretary of Defense*. Washington, DC: Department of Defense.

[7] Since at least 2008, CE has been defined simply as "reviewing the background [of covered personnel] at any time during the period of eligibility to determine whether that individual continues to meet the requirements for eligibility" (Exec. Order No. 13467, 73 Fed. Reg. 128 [July 2, 2008]). In practice, however, it has been more closely associated with the "CE System" of automated records checks established by the Office of the Director of National Intelligence.

[8] Inspector General. (October 15, 2015). *DoD needs a comprehensive approach to address workplace violence* (Report DODIG-2016-002). Washington, DC: Department of Defense.

[9] Department of Defense. (2014). *DoD workplace violence prevention response and policy* [DoD Instruction 1438.06]. Washington, DC: Author.

the Under Secretary of Defense for Personnel and Readiness told DoDIG that a distinct workplace violence policy for military personnel had not been developed because it was believed that the Uniform Code of Military Justice (UCMJ) "was sufficient to assist commanders when they addressed military personnel's 'bad behavior' in the workplace" (p. 14). DoDIG warned, however, that relying solely on UCMJ's disciplinary authorities to address potential workplace violence risks could be counterproductive when responding to signs of escalating threats.

Likewise, DoDIG found that no workplace violence prevention and response policies existed for the contractor workforce. In response, DoD noted that the 2010 Fort Hood Independent Review scope had been limited to military and civilian personnel. DoDIG pointed out that the Fort Hood reports did, however, "strongly recommend" that contractor policies should be reviewed in the future.[10] Despite all of these gaps in DoD-level policies, DoDIG did find that many Components had begun to implement workplace violence prevention and response programs using different approaches drawn from various reports and policy memoranda in order to address specific organizational needs.

The Counter-Insider Threat Mission

While the workplace violence policy landscape rapidly shifted, and as a result of the 2010 WikiLeaks incident, then-President Barack Obama issued Executive Order (E.O.) 13587 in 2011 which began the formal effort to deter, detect, and mitigate insider threats to classified information within the Executive Branch.[11] E.O. 13587 established the National Insider Threat Task Force (NITTF) to develop policy and standards for the "safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure."

In 2012, the Obama administration issued the *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs* (hereinafter, *Minimum Standards*).[12] These standards defined insider threat as the risk of harm to national security by those with authorized access to classified information. Among a number of other requirements, the *Minimum Standards* mandated user activity monitoring and "continued evaluation" programs, but limited their applicability to individuals with access to classified systems and information. Much like a TMU model, the *Minimum Standards* took a multidisciplinary approach to gathering, integrating, analyzing, and responding to threats, and specifically mandated information-sharing across agencies. They also required Federal agencies to establish their own procedures for information-sharing and referrals across multiple disciplines. However, they did not address specific methods of incident response or risk mitigation.

DoD established its Counter-Insider Threat Program (C-InTP) officially in 2014.[13] The DoD C-InTP policy required all 44 DoD Components to implement the *Minimum Standards* and "establish or maintain" their own programs based on "a multi-disciplinary threat management capability to conduct and integrate the monitoring, analysis, reporting, and response to insider threats" (p. 13). The policy required Components to ensure that multidisciplinary teams made up of experts from law enforcement, counterintelligence, mental health, security, civilian and military personnel management, general counsel, and cybersecurity be available to all commanders (or civilian

[10] Department of Defense Independent Review Related to Fort Hood. (2010). p. 11.
[11] Exec. Order No. 13587, 76 Fed. Reg. 63811 (October 7, 2011).
[12] Presidential Memorandum. (November 21, 2012). *National insider threat policy and minimum standards for Executive Branch insider threat programs*. The White House: Office of the Press Secretary.
[13] Department of Defense. (2014). *The DoD Insider Threat Program* [DoD Directive 5205.16]. Washington, DC: Author. The label "Counter-Insider Threat Program" has since been adopted by DoD to better reflect its mission, and is used here in anticipation of its formal inclusion in DoD policy.

equivalents). However, DoD C-InTP policy did not establish operating guidance for Component programs at that time.

The 2014 DoD C-InTP policy expanded the covered population beyond the *Minimum Standards* to include all DoD personnel with national security eligibility, not just those with authorized access to classified information. In effect, this made the program applicable to all military personnel as well as civilian and contractor personnel who "[have] or had" been granted national security eligibility (p. 16).

In 2015, a DoDIG assessment of Component programs identified a number of problems with policy implementation.[14] Most significantly, the assessment found that implementation had been highly inconsistent across Components. Because DoD policy lagged behind Executive Branch insider threat directives, many Components had begun to develop their own programs in the interim based on their unique missions and the specific threats they faced. Other Components had delayed implementation altogether in the absence of DoD-level guidance and dedicated resources.

Development of PAR Capabilities

In 2017, after a number of high-impact insider threat attacks on both DoD personnel and data, and in the midst of a rapidly changing policy environment, DoD issued the PAR Memo. Originally, DoD planned to require TMUs in line with recommendations from the 2010 Fort Hood Independent Review, the 2012 DSB study, and the 2013 Navy Yard Review, but Components resisted these plans over concerns about resources and available funding.[15]

The resulting PAR Memo represented a significantly scaled-down compromise. Much like a TMU model, PAR capabilities relied on a multidisciplinary team of "professionally trained and qualified personnel" assigned to "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." Unlike a TMU, however, PAR would not be staffed by a dedicated team; instead, members would be drawn from an installation's existing support functions. The PAR Memo included "no requirement to create any new capability" and left Components to "utilize existing capabilities to the maximum extent possible" (pp. 1-2).

The PAR Memo set two objectives that reflected existing gaps between DoD's violence prevention and counter-insider threat policies. First, PAR capabilities would apply to the entire DoD workforce "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." Second, the PAR Memo acknowledged that effective risk assessment and mitigation capabilities could not be isolated from other, similar efforts. Thus, it directed that PAR's risk assessment and mitigation capabilities should "align with and complement" DoD and Component C-InTPs (pp. 1-2).

[14] Inspector General. (September 29, 2015). *Assessment of the Military Services' insider threat programs* (Report DODIG-2015-184 REDACTED). Washington, DC: Department of Defense. Retrieved from https://fas.org/irp/agency/dod/ig-insider.pdf

[15] Office of the Under Secretary of Defense for Intelligence, personal communication, November 15, 2018.

Recent PAR-Related Policy Developments

Four major Congressional or Executive policy actions came into effect after the 2017 PAR Memo was written, each of which further reinforces the need to align workplace violence and the C-InTP. First, Congress radically revised the definitions of insiders and the threats they pose to DoD in the National Defense Authorization Act (NDAA) for 2017.[16] The NDAA 2017 expanded the definition of insider to include the entire DoD population, a move that had been a primary objective of PAR. It also expanded the DoD C-InTP mission beyond protecting classified information and systems, and effectively merged the counter-insider threat mission with the workplace violence prevention mission. Second, the NDAA 2017 clarified the authorities to collect, store, and retain information by DoD and Component C-InTPs. Based on these new authorities, the DoD C-InTP updated its system of records notice to allow for more effective information-sharing for multidisciplinary threat assessment and mitigation.

A third policy change has not yet been fully realized but will have long-term effects on both Component C-InTPs and PAR capabilities. A January 2017 revision to Federal suitability, fitness, and national security eligibility rules by the Obama administration established a single integrated vetting enterprise to cover the entire Executive Branch workforce.[17] The new rules defined vetting in a way that merged determinations for national security eligibility, employment suitability and fitness, and even military service eligibility into a common framework. In a significant departure from decades of Federal and DoD policies, the new framework would be built around continuous vetting (CV), an end-to-end process applicable to the entire Federal workforce that included background investigations, adjudications, and ongoing assessments throughout an individual's government employment. While existing CE programs remained intact, the CV framework that is built on these capabilities should drive future efforts across Federal agencies to better integrate personnel security and human resources in the development of a trusted workforce.

Finally, Congress prioritized program integration in the NDAA 2018, and directed DoD to develop plans to "fully integrate insider threat data, tools, and capabilities into the new end-to-end vetting process . . . to ensure a holistic and transformational approach to detecting, deterring, and mitigating threats posed by trusted insiders."[18] In other words, workplace violence prevention, counter-insider threat, and personnel vetting policies formally converged.

Discussion

The convergence of workplace violence prevention, the counter-insider threat mission, and personnel security policy has led stakeholders from across DoD to move the substantive content of their workforce protection efforts toward a common endpoint, which is so far best expressed in the PAR Memo. The PAR concept evolved from DoD efforts to address the realities of internal threats in the midst of a rapidly changing policy environment, and reminded stakeholders that in most insider threat cases there are behavioral indicators that, if reported, could be acted on to mitigate risks before they escalate. Because of this, the PAR Memo needed to establish links between workplace violence and insider threat prevention due to policy limitations that, at the time it was written, prevented C-InTPs from collecting, analyzing, or sharing information on non-cleared personnel. At

[16] National Defense Authorization Act for fiscal year 2017, Pub. L. No. 114-328 § 951, 130 Stat. 2371 (2016).
[17] Exec. Order No. 13764, 82 Fed. Reg. 13 (January 23, 2017).
[18] National Defense Authorization Act for fiscal year 2018. Pub. L. No. 115-91 § 925, 131 Stat. 1526 (2017).

the same time, the growing consensus between behavioral science researchers and C-InTP practitioners on the applicability of behavioral precursors to a range of potentially harmful behaviors reflected the urgency to find effective means of threat prevention.

Within this institutional context the PAR Memo was perhaps both inevitable and inevitably imperfect. While clearly a move in the right direction, it was unable to anticipate continuing policy changes, which have been too often incrementally driven by events rather than by overarching strategic objectives. In hindsight it is hard not to conclude that a 6-month delay in the PAR Memo's release would have resulted in a very different policy document. Given this and the current state of PAR and C-InTP development, DoD leaders should work to fully integrate their ongoing efforts to build effective workplace violence, counter-insider threat, and personnel vetting programs within a comprehensive threat prevention strategy to protect the DoD workforce.