Report on Countering Extremist Activity Within the Department of Defense

December 2021

"The overwhelming majority of the men and women of the Department of Defense serve this country with honor and integrity. They respect the oath they took to support and defend the Constitution of the United States. We are grateful for that dedication… ***We owe the men and women of the Department of Defense an environment free of extremist activities, and we owe our country a military that reflects the founding values of our democracy."***

Secretary of Defense Lloyd J. Austin III
Memorandum, December 20, 2021

EXECUTIVE SUMMARY

This report outlines ongoing work by the Department of Defense to address the threat posed by prohibited extremist activities. The Department of Defense has long prohibited Service members from actively engaging in extremist activities. Since 1969, the Department of Defense has provided policy guidance that enumerates the prohibition of specific activities, and has routinely updated its guidance to clarify prohibited activities, clarify the investigative authorities that commanders have at their disposal, and ensure that all military departments implement training on these policies.

Following a number of high-profile insider threat attacks in the early 2010s, the Department of Defense built a program to detect, deter, and mitigate such threats to the Department, its people, and its mission. In 2019, Congress directed the Department of Defense to review existing policies and capabilities with the aim of closing gaps in personnel security vetting. In 2020, the Army published a comprehensive revision of Army Command Policy (AR 600-20) which was the first of its kind to address the use of social media to support extremist activities and provided guidance to commanders for addressing prohibited activity that crosses the line into misconduct.

In February 2021, Secretary of Defense Lloyd J. Austin III directed a Department-wide stand down to educate Department of Defense personnel on the threat posed by extremist activity. In April 2021, following the stand down, Secretary Austin issued a second memorandum to implement immediate actions identified by subject-matter experts within the Department of Defense (and informed by the stand down), and directed the establishment of the Countering Extremist Activity Working Group (CEAWG) to implement these urgent steps and develop additional recommendations.

This report provides background on the work completed by the Department. It also details the implementation status of the Secretary's four directed actions from April and describes the six additional recommendations and associated actions developed by the CEAWG. With the publication of this report, the Secretary of Defense has directed the implementation of the six CEAWG recommendations and associated actions.

The immediate actions were:

- Review and update DoD Instruction 1325.06, "Handling Protest, Extremist, and Criminal Gang Activities Among Members of the Armed Forces," to clarify the definition of prohibited extremist activity
- Update the Service member transition checklist
- Review and standardize screening questionnaires
- Commission a study on extremist activity in the Total Force.

The six additional CEAWG recommendations fall within the following lines of effort: Military Justice and Policy, Support and Oversight of the Insider Threat Program, Investigative Processes and Screening Capability, and Education and Training. Key recommendations include:

- Developing a comprehensive training and education plan that provides regular training on prohibited extremist activity to Department of Defense personnel, including those advancing to leadership positions.
- Reviewing and updating policies to provide notice to the Total Force and Department of Defense contractor personnel on prohibited extremist activity.
- Improving and modernizing Insider Threat programs by enhancing capabilities, maximizing information sharing, and ensuring a consistent and full understanding of any legal requirements.

1. INTRODUCTION

At the direction of Secretary of Defense Lloyd J. Austin III, the Department of Defense (DoD) is addressing the threat posed by prohibited extremist activities, and taking steps to ensure that Service members, DoD civilian employees, and all who support the Department's mission can serve in a secure environment free from discrimination, hatred, and harassment.

Countering Domestic Terrorism

In 2020, both the Federal Bureau of Investigation and the U.S. Department of Homeland Security found that a range of extremist motivations and behaviors constituted a growing threat to the United States. On June 15, 2021, the Biden Administration released the first-ever National Strategy for Countering Domestic Terrorism to address the security challenge posed by domestic terrorism. The report followed a 100-day comprehensive review of U.S. efforts to address domestic terrorism. Upon its release, the White House noted in a fact sheet:

> Domestic terrorism is not a new threat in the United States, yet it is a threat Americans have endured too often in recent years. The comprehensive strategy provides a nationwide framework for the U.S. Government and partners to understand and share domestic terrorism related information; prevent domestic terrorism recruitment and mobilization to violence; disrupt and deter domestic terrorism activity; and confront long term contributors to domestic terrorism. Our approach will protect both the nation and the civil liberties of its citizens.

The Department of Defense's policies and programs related to countering extremist activity correlate with the National Strategy. The efforts of the Department of Defense's CEAWG primarily fall within National Strategy Pillars Three (Disrupt and Deter Domestic Terrorism Activity) and Four (Confront Long-Term Contributors to Domestic Terrorism).

Background on the Prohibition of Extremist Activity in the Armed Forces

Since 1969, the Department of Defense has provided policy guidance that enumerates the prohibition of specific activities by members of the Armed Forces. Over the subsequent five decades, that guidance has been routinely updated in response to significant events. In 1986, in response to the White Patriot Party's weapons theft incident, the guidance was updated with an addition of "prohibited activities." Later in the mid-1990s, following a series of high profile incidents, additional points were added to clarify the investigative authorities that commanders had at their disposal while also ensuring that all military departments implemented training on these policies.

Following a number of serious insider threat attacks in the early 2010s, the Department built a program to detect, deter, and mitigate such threats to the Department, its people, and its mission. In 2019, Congress directed the Department to review existing policies and capabilities

with the aim of closing gaps in personnel security vetting pertaining to the use of web-based platforms by those who promote extremist or criminal gang activities. In 2020, the Army published a comprehensive revision of Army Command Policy (AR 600-20) which was the first of its kind to address the use of social media to support extremist activities and provided guidance to commanders for addressing prohibited activity that crosses the line into misconduct. These issues have also been addressed in numerous Executive Orders, Titles 10 and 18 of the United States Code, and several National Defense Authorization Acts.

The overall intent of these policies has been to provide guidance to commanders and guidelines for military personnel regarding prohibited and dangerous activities — including violence, actions that undermine good order and discipline, and the inequitable treatment of Service members.

Secretary of Defense Directed Actions

Since his appointment, Secretary Austin has issued two memoranda to guide the Department's response to the threat posed by extremist activity. The first directed a Department wide "stand-down" to educate personnel across the Total Force, and the second directed a set of immediate actions and the establishment of the CEAWG.

On February 5, 2021, Secretary Austin released a memorandum entitled "Stand-Down to Address Extremism in the Ranks." It outlined the importance of the constitutionally required oath of office for all members of the Total Force and underscored the incompatibility of extremist activities with that oath. The memorandum also directed commanding officers and supervisors across the Total Force within sixty days to conduct a one-day "stand-down," using the Department of Defense instruction that describes prohibited extremist activities (DoDI 1325.06) as a guiding document for "stand-down" discussions. Secretary Austin directed these discussions to include "the importance of our oath of office; a description of impermissible behaviors; and procedures for reporting suspected, or actual, extremist behaviors in accordance with the DoDI." Secretary Austin also directed leaders to listen to the "concerns, experiences, and possible solutions" from the workforce during these discussions.

On April 9, 2021, Secretary Austin released a memorandum which directed a series of immediate actions and the establishment of a cross-functional working group (the CEAWG) to oversee the implementation of the immediate actions and the formulation of additional mid-term and long-term recommendations. The immediate actions directed by Secretary Austin included:

- Review and update DoDI 1325.06 to clarify the definition of prohibited extremist activity
- Review and standardize accession questionnaires
- Update the Service member transition checklist
- Commission an outside study on extremist activity in the Total Force

The following sections of this report include: an overview of the CEAWG's purpose, approach, and actions; updates on the status of the four immediate actions directed by the Secretary's April 9, 2021, memorandum; and the CEAWG's six additional recommendations and their associated actions.

Overview of the Countering Extremist Activity Working Group

Secretary Austin directed the CEAWG to oversee the implementation of four immediate actions and the development of recommendations across four lines of effort. The CEAWG's work was informed by both internal and external subject-matter experts and coordinated with other Federal departments and agencies. It was grounded in rigorous research, data, and lessons learned from the Department's stand-down in the spring of 2021.

Secretary-Directed Lines of Effort

- **Line of Effort 1: Military Justice and Policy**. This line of effort evaluated amending the Uniform Code of Military Justice (UCMJ), and amending related Department policy, to address extremist activity.
- **Line of Effort 2: Support and Oversight of the Insider Threat Program**. This line of effort determined how the Department could better collect and share information among the Military Service Insider Threat Programs, law-enforcement organizations, security organizations, and commanders and supervisors—all consistent with Pillar 1 of the National Strategy ("Understand and Share Domestic Terrorism-Related Information"). This line of effort focused on strengthening Insider Threat Programs and the Direct Awareness Campaign with the goal of promoting the use of the Insider Threat programs to report concerning activities by military and civilian personnel.
- **Line of Effort 3: Investigative Processes and Screening Capability**. This line of effort examined the Department's pursuit of scalable and cost-effective capabilities to improve the screening of publically available electronic information (PAEI) as part of background investigations. PAEI — information available to the public on an electronic platform such as a website, social media outlet, or database — can be a unique data source to identify security concerns under the Federal National Security Adjudicative Guidelines, which establish the common criteria for determining eligibility for access to classified information or for holding a sensitive position.
- **Line of Effort 4: Education and Training**. This line of effort used the CEAWG review to update counter extremist activity and Insider Threat training at all leadership levels. It applied lessons from the stand down to make recommendations of how to improve training and education, including the incorporation of the revised DoDI 1325.06 definition of prohibited extremist activity.

CEAWG Structure

The CEAWG included a steering committee and subcommittees for each line of effort. The CEAWG Steering Committee comprised senior members of the Office of the Under Secretary of Defense for Personnel and Readiness, the Office of the Under Secretary of Defense for Intelligence and Security, the Office of the General Counsel of the DoD, the Joint Staff, and liaisons from each Military Service. This steering committee provided regular updates to, and received guidance and direction from, the Workforce Management Group (WMG) and, ultimately, the Deputy's Workforce Council (DWC).

Data Analysis

The CEAWG incorporated quantitative and qualitative data from internal and external experts to help inform this report, including:

- A briefing from the University of Maryland National Consortium for the Study of Terrorism and Responses to Terrorism (START)
- A briefing from the West Point Cyber Security Institute
- Analysis of internal Military Justice data and FBI cases
- External listening sessions with Military Service Organizations, Veterans' Service Organizations, think tanks, civil-rights organizations, and institutions of higher education

The available data generally shows that cases of prohibited extremist activity among Service members was rare. However, even a small number of cases can pose a significant problem, challenging safety and unit cohesion. START data indicated recent spikes in the instances of domestic violent extremism, and an uptick in veteran participation in these cases.

The Department's ability to track instances of prohibited extremist activity across multiple databases such as the DoD IG case management system, Military Criminal Investigative Service systems, military justice systems, and Military Equal Opportunity systems has improved since 2018 due to the introduction of systems for flagging instances that are assessed to constitute prohibited extremist activity. Combined with better processes for reporting command-level incidents up to a Service-level organization, flagging systems such as checkboxes, radio buttons, or drop down menus provide better tracking mechanisms of prohibited extremist activity across the Department.

As a result of those process improvements, the Department of Defense has determined the number of substantiated matters of members of the military who are subject to official action due to engagement in prohibited extremist activity are fewer than 100 over the past year. Substantiated instances may be increasing over time, although comparisons with prior years is challenging due to inconsistent data collection as system flags were introduced along different timelines beginning in 2018. There are opportunities to enhance standardization and communication between systems for more consistent data tracking across the Department, which will lead to greater fidelity. This need is addressed by the CEAWG recommendations,

particularly Recommendations 1 and 4, which focus on program enhancements to the Defense Insider Threat Management and Analysis Center (DITMAC) and the DoD Inspector General's case management system, the Defense Case Activity Tracking System-Enterprise (D-CATSe).

2. IMMEDIATE ACTIONS TO COUNTER PROHIBITED EXTREMIST ACTIVITIES

This section provides the status of each immediate action directed by Secretary Austin's April 9, 2021 memorandum.

Immediate Action 1: Review and Update of DoD Instruction 1325.06 Definition of Extremist Activity

The Under Secretary of Defense for Personnel and Readiness (USD(P&R)) and the Office of the General Counsel (OGC) of the DoD will review and update DoDI 1325.06 to revise its definition of prohibited extremist activities among uniformed military personnel. In parallel with the DoDI 1325.06 update, the USD(P&R), in consultation with the OGC, will consider policy recommendations and options to address extremist activity by and among DoD civilian employees and contractors.

Task 1.1. Review and Update Definition of Extremist Activity in DoDI 1325.06

Office of Primary Responsibility: USD(P&R)
Status: Complete

Prior to its recent amendment, DoD Instruction 1325.06 prohibited Service members from "active advocacy" of "supremacist, extremist, or criminal gang doctrine, ideology, or causes, including those that advance, encourage, or advocate the use of force, violence, or criminal activity or otherwise advance efforts to deprive individuals of their civil rights." Service members were further directed to reject "active participation" in organizations that do the same.

Feedback from the 2021 Department wide stand down demonstrated a need to clarify the DoDI 1325.06 phrase "active participation." Additionally, the Military Departments sought clarification regarding social-media activity, for which Congress directed the Department to establish training programs in the FY21 National Defense Authorization Act.

The CEAWG concluded that DoDI 1325.06 needed to be revised to more clearly define the terms "extremist activities" and "active participation." The group also recommended that the revisions emphasize the importance of the role of commanders and address online activities.

Revisions to DoDI 1325.06, including definitions of "extremist activities" and "active participation" were thoroughly coordinated with the Military Departments and other DoD Components. The revised instruction identifies harms to the military from extremist activities, discusses the authority of the commander to maintain good order and discipline, and lists activities that are prohibited by members of the Armed Forces.

DoDI 1325.06 (Excerpt)

(1) Extremist Activities. The term "extremist activities" means:

(a) Advocating or engaging in unlawful force, unlawful violence, or other illegal means to deprive individuals of their rights under the United States Constitution or the laws of the United States, including those of any State, Commonwealth, Territory, or the District of Columbia, or any political subdivision thereof.

(b) Advocating or engaging in unlawful force or violence to achieve goals that are political, religious, discriminatory, or ideological in nature.

(c) Advocating, engaging in, or supporting terrorism, within the United States or abroad.

(d) Advocating, engaging in, or supporting the overthrow of the government of the United States, or any political subdivision thereof, including that of any State, Commonwealth, Territory, or the District of Columbia, by force or violence; or seeking to alter the form of these governments by unconstitutional or other unlawful means (e.g., sedition).

(e) Advocating or encouraging military, civilian, or contractor personnel within the DoD or United States Coast Guard to violate the laws of the United States, or any political subdivision thereof, including those of any State, Commonwealth, Territory, or the District of Columbia, or to disobey lawful orders or regulations, for the purpose of disrupting military activities (e,g., subversion), or personally undertaking the same.

(f) Advocating widespread unlawful discrimination based on race, color, national origin, religion, sex (including pregnancy), gender identity, or sexual orientation.

(2) Active Participation. For purposes of this section, the term "active participation" means the following, except where such activity is within the scope of an official duty (e.g., intelligence or law enforcement operations):

(a) Advocating or engaging in the use or threat of unlawful force or violence in support of extremist activities.

(b) Advocating for, or providing material support or resources to, individuals or organizations that promote or threaten the unlawful use of force or violence in support of extremist activities, with the intent to support such promotion or threats.

(c) Knowingly communicating information that compromises the operational security of any military organization or mission, in support of extremist activities.

(d) Recruiting or training others to engage in extremist activities.

(e) Fundraising for, or making personal contributions through donations of any kind (including but not limited to the solicitation, collection, or payment of fees or dues) to, a group or organization that engages in extremist activities, with the intent to support those activities.

(f) Creating, organizing, or taking a leadership role in a group or organization that engages in or advocates for extremist activities, with knowledge of those activities.

(g) Actively demonstrating or rallying in support of extremist activities (but not merely observing such demonstrations or rallies as a spectator).

(h) Attending a meeting or activity with the knowledge that the meeting or activity involves extremist activities, with the intent to support those activities:

(1) When the nature of the meeting or activity constitutes a breach of law and order;

(2) When a reasonable person would determine the meeting or activity is likely to result in violence; or

(3) In violation of off-limits sanctions or other lawful orders.

(i) Distributing literature or other promotional materials, on or off a military installation, the primary purpose and content of which is to advocate for extremist activities, with the intent to promote that advocacy.

(j) Knowingly receiving material support or resources from a person or organization that advocates or actively participates in extremist activities with the intent to use the material support or resources in support of extremist activities.

(k) When using a government communications system and with the intent to support extremist activities, knowingly accessing internet web sites or other materials that promote or advocate extremist activities.

(l) Knowingly displaying paraphernalia, words, or symbols in support of extremist activities or in support of groups or organizations that support extremist activities, such as flags, clothing, tattoos, and bumper stickers, whether on or off a military installation.

(m) Engage in electronic and cyber activities regarding extremist activities, or groups that support extremist activities – including posting, liking, sharing, re-tweeting, or otherwise distributing content – when such action is taken with the intent to promote or otherwise endorse extremist activities. Military personnel are responsible for the content they publish on all personal and public Internet domains, including social media sites, blogs, websites, and applications.

(n) Knowingly taking any other action in support of, or engaging in, extremist activities, when such conduct is prejudicial to good order and discipline or is service-discrediting.

Task 1.2. Consider Policy Recommendations to Address Extremist Activities by and Among DoD Civilian Employees and Contractor Personnel

Office of Primary Responsibility (Civilian Policy): USD(P&R)
Office of Primary Responsibility (Contractor Policy): USD(A&S)
Status: 90 days from date of publication of revised DoDI 1325.06

The stand down surfaced concerns that the Department may be underemphasizing the civilian oath of office and that departmental policy on prohibited extremist activity for civilian employees and contractor personnel is underdeveloped. With the publication of DoDI 1325.06, the USD(P&R), in consultation with the Office of Personnel Management (OPM), will develop recommendations for updating policy applicable to Department of Defense civilian employees. The Under Secretary of Defense for Acquisition and Sustainment will develop similar policy options for Department of Defense contractor personnel.

Immediate Action 2: Update Service Member Transition Checklist.

The Secretaries of the Military Departments will add provisions to their Service member transition checklists for individuals separating or retiring from the military that include training on potential targeting of Service members by extremist groups and work with other federal departments and agencies to create a mechanism by which Veterans have the opportunity to report any potential contacts with an extremist group should they choose to do so.

Task 2.1. Update Service Member Transition Checklist

Office of Primary Responsibility: USD(P&R)
Office of Secondary Responsibility: Military Services
Status: Complete

Under the USD(P&R), the Military-Civilian Transition Office (MCTO) added language to the DoD Transition Assistance Program (TAP) Pre-Separation Counseling Script that reinforces the key messages from the stand down and underscores the need to honor the oath of office and to support and defend the Constitution. The new script provides various law-enforcement reporting methods for extremist activities, including the FBI's Tip Form and how to make reports to local FBI and police or sheriffs' departments. The Military Services have made implementation of the new script a part of mandatory counseling before leaving the military. MCTO will review, revise, and publish the script at the end of each Fiscal Year, as appropriate.

While the Military Departments have begun updating their own transition training resources, they expressed a need for Department wide, standardized, transition-training resources on extremist activity. Consequently, a single Joint Knowledge Online (JKO)-based training on extremist activity is being established to broadly cover the topic of responding to recruiting efforts by violent extremist groups during the transition period. The course will include information to prepare Service members if they face such recruitment efforts after their military service ends. It will also include an advisory for Service TAP programs to refer individuals, as appropriate, to the FBI Tip Line (Online Tip and Public Leads portal, Internet Crime Complaint

Center, or via phone at 1-800-225-5324). Military Services are directed to use this training as part of their recurring mandatory trainings and report completion to the USD(P&R).

Task 2.2. Multi-Department and Interagency Coordination to Support Veterans in Guarding Against Recruitment by Extremist Groups

Office of Primary Responsibility: USD(P&R)
Status: Ongoing

The CEAWG regularly engaged Department of Veterans Affairs (VA) Department of Homeland Security (DHS), Office of Personnel Management (OPM), and U.S. Intelligence Community (IC) subject-matter experts throughout its deliberations. The Department of Defense continues to explore ways to do more with existing joint working groups within each agency to advance common research interests, goals, and procedures for joint efforts to counter extremist activity and enable Veterans to guard against recruitment by extremist groups.

The Department of Defense and the VA have engaged in several information sharing sessions to review best practices from the Department of Defense's directed stand down; further understand the role of mental and behavioral health in extremist activity; share updated accession forms and questionnaires; and examine the impact of criminal actions that may affect a characterization of service for the purpose of accessing VA services and benefits. Most veterans are not subject to court-martial jurisdiction, and as such, the VA is the agency responsible for executing any termination of Veterans' benefits based on civilian prosecution.

The Department of Defense will continue to engage in partnership efforts with the VA, DHS, OPM, and IC to inform and coordinate training, education, and best practices to ensure continuity of approach between the agencies wherever practicable.

Immediate Action 3: Review and Standardization of Screening Questionnaires.

The Secretaries of the Military Departments will update and standardize accession screening questionnaires to solicit specific information about current or previous extremist activity. Such questions should be designed: 1) to gather actionable information in the short term to ensure that only the best qualified recruits are selected for services, and 2) to clarify that any demonstrably false answers provided in response could form the basis for punitive action for fraudulent enlistment.

Office of Primary Responsibility: Military Services
Office of Secondary Responsibility: USD(P&R) and USD(I&S)
Status: Complete

In recent years, several tragic incidents involving people with access to Department of Defense installations have underscored the profound importance of personnel screening and security. These include the 2009 Fort Hood shooting, the 2013 Washington Navy Yard massacre, and the 2019 Joint Base Pearl Harbor-Hickam and Pensacola Naval Air Station shootings.

As directed by Immediate Action 3 in Secretary Austin's April 9, 2021, memorandum, the Military Services updated their accession screening forms throughout the spring of 2021 to include questions on membership in racially biased entities and other extremist groups, as well as participation in violent acts. The forms emphasize that engaging in criminal gangs, extremist organizations, and associated activities is strictly prohibited. This afforded USD(P&R) and USD(I&S) time to develop a standardized battery of questions for use across all Military Services to ensure consistency across recruiting operations and data collection.

Over the summer of 2021, the Department established procedures to incorporate FBI review of questionable tattoos and branding that suggest propensities to extremism and violence through the FBI Cryptology and Racketeering Records Unit. A partnership with the FBI now allows recruiting commands and the Military Criminal Investigative Organizations (MCIOs) access to the FBI's Law Enforcement Enterprise Portal (LEEP), offering a wide range of information on local gangs, white-supremacy and nationalist groups, gang signs, and extremist symbols and tattoos. A positive declaration to the accession screening forms or tattoo correlation with the LEEP requires an approved Morals Eligibility Determination (e.g., accession waiver) by Service senior leadership to continue processing an applicant for entry into the Armed Forces.

Immediate Action 4: Commission a Study on Extremist Activity within the Total Force (Armed Service personnel, DoD civilian personnel, and contractors)

The Department will commission a study on extremist activity within our Total Force, to include gaining greater fidelity on the scope of the problem.
Office of Primary Responsibility: USD(P&R)
Status: Complete; Final Report Anticipated June 2022

The Department chartered the Institute for Defense Analyses (IDA) to work with the Defense Personnel and Security Research Center to conduct a comprehensive study of extremist activity across the Total Force. The scope of work includes three phases:

1. *Phase I* – A review of common frameworks, research, and recommendations for the DoD Total Force (e.g., U.S. Law, Adjudicative Standards for National Security Positions).

2. *Phase II* – A review of DoD information-collection systems and data, approaches used for other forms of violence by other federal agencies, and behavioral pathways to extremist activity.

3. *Phase III* – Development of recommendations pertaining to military forces and to DoD civilian personnel and contractor employees.

The research includes a review of published literature and internal Department of Defense data, law, policy, practices, and procedures. It also includes an overview of nongovernmental organizations, viewpoints from internal and external experts, consultations with law-enforcement experts, intelligence experts, insider-threat experts, threat assessors, and authoritative data documenting extremist behavior and activity. IDA has completed Phase I and Phase II of the study, and the Phase III research is well underway. The final report is anticipated in June 2022.

Several other relevant studies are also underway, including:

- Research by the Applied Research Laboratory for Intelligence and Security (ARLIS), a Department of Defense sponsored University Affiliated Research Center, to provide independent testing and evaluation of approaches to collecting relevant data for background investigations.
- Expanding research at the University of Maryland's START to focus more precisely on hate crimes and other violence by military or military-affiliated personnel that fall below the domestic-terrorism threshold. This will include additional datasets to enable agile data collection to anticipate and answer future extremism-related questions.
- A partnership between National Defense University (NDU) and the Joint Staff to review patterns of recruitment by extremist groups of U.S. military and affiliated personnel and explore potential interventions.

3. ADDITIONAL RECOMMENDATIONS

The CEAWG also provided recommendations in the areas of Military Justice and Policy, the Insider Threat Program, Investigative Processes and Screening Capabilities, and Education and Training. USD(P&R) and USD(I&S) will oversee the implementation of the following initiatives and associated actions with quarterly reports to the Deputy Secretary of Defense, through the Deputy's Workforce Council (DWC).

1. Identify funding required for key areas related to insider-threat (InT) analysis and response, including:

(1.1) A centralized Prevention, Assistance, and Response (PAR) capability that standardizes implementation of Insider Threat program requirements and reduces DoD Component concerns about organizational responsibilities and resourcing requirements.

(1.2) A centralized Behavioral Threat Analysis Center (BTAC), staffed by behavioral science and threat-assessment/management personnel to support the DoD Insider Threat program.

(1.3) A robust Defense Insider Threat Management and Analysis Center (DITMAC) System of Systems capability to enhance case-management capabilities and advanced analytics to identify trends.

(1.4) An Insider Threat Assessment Program through the DITMAC's Enterprise Program Management Office (EPMO). New EPMO personnel will evaluate all DoD InT programs based on appropriate risk-management criteria outlined in the "enhanced FOC" document.

(1.5) A DoD Workforce InT hotline to create a Department-wide virtual, anonymous reporting capability, and triage management center.

(1.6) A DoD InT Program funding line for the DoD Insider Threat program.

(1.7) Support of the DoD Inspector General, through the Deputy Inspector General for Diversity, Inclusion, and Extremism (DIEM), consistent with Section 554 of the FY 2021 National Defense Authorization Act (NDAA).

2. Develop a comprehensive training and education plan that provides regular training to Department of Defense military and civilian personnel and to those advancing to leadership positions. The plan will cover factors such as content, periodicity, and modality. At a minimum, content will be based on the new definition of "extremist activities" and "active participation" contained in the revised DoDI 1325.06, to include reporting options, and available resources. This DoD-wide training on extremist activity and InT education plan will include:

(2.1) Evaluating and implementing best methods and curriculum for leadership training on Insider Threat and Prevention, Assistance, and Response (PAR) resources within 240 days.

(2.2) Creating a new annual, stand-alone, computer-based Joint Force extremist activity training course for delivery in FY22 based on the revised DoDI 1325.06 definition.

(2.3) Sharing information and best practices on countering extremist activity with international allies and partners through existing engagements.

(2.4) Developing a combined InT awareness and countering extremist activities training, and a requirement for the Services to include this training in all levels of Professional Military Education.

(2.5) Requiring the Services to include in-person discussions about extremist activity in periodic training addressing unit climate and culture to amplify education efforts, allow feedback to inform future efforts and understanding, and strengthen organizational culture and climate.

(2.6) Requiring the Services to develop counter-extremist activity training tailored for Senior Enlisted Leaders (SELs), law enforcement, recruiters, and legal advisors.

3. Review and update relevant policies to provide notice to Total Force personnel concerning prohibited activities. This will include establishing policy and a definition of "extremist activity" applicable to DoD civilian employees to be included in DoDI 1438.06, "*DoD Workplace Violence Prevention and Response Policy,*" within 90 days of the publication of the revised extremist activities definition in DoDI 1325.06. As the Department develops this new definition applicable to civilian personnel, it will be aligned as closely as possible to the revised definition applicable to military personnel.

(3.1) After a definition of prohibited extremist activities for civilian personnel is established, OUSD(P&R) will reissue DoDI 1438.06, draft or reissue any other relevant

policy, and develop any necessary training materials to establish clear standards for Department of Defense civilian employees concerning prohibited extremist activity.

(3.2) Examining the possibility of including extremist behavior in the adjudicative criteria for suitability determinations under DoDI 1400.25 Volume 731, "*DoD Civilian Personnel Management System: Suitability and Fitness Adjudication for Civilian Employees*," to allow for a civilian employee's extremist activity to be included as part of DoD's determination of their suitability.

(3.3) Utilizing existing force-protection and base-security authorities to address extremist activities and threats pursuant to DoDI 5200.08, "Security of DoD Installations and Resources and the DoD Physical Security Review Board," with regard to DoD contractor personnel.

(3.4) Utilizing existing contracting officer authorities to ensure compliance with the terms and conditions of DoD contracts.

(3.5) Designating the USD(I&S) as the OSD PSA proponent for the InT Program's Prevention, Assistance, and Response (PAR) policy, integrating it with the larger InT capability planning and operations, and publishing the PAR implementation policy within 180 days.

(3.6) Evaluating the transition of workplace violence policy to OUSD(I&S), to further synchronize that policy with the InT program and PAR policies, and implementing the decision within 180 days.

4. Insider Threat study on information sharing and risk prioritization. This study will:

(4.1) Compare information reported to the DITMAC, and evaluate it against information reported through personnel security, counterintelligence, and law enforcement channels.

(4.2) Determine whether reported information leads to appropriate responses and whether relevant information is reaching insider-threat hubs.

(4.3) Determine whether, and if so, what specific statutory authority may be necessary to increase both reporting and availability of data to insider-threat hubs.

(4.4) Assess and recommend any technical capabilities that could assist hubs in prioritizing work based on risk.

5. Improve and modernize the Insider Threat program to create clear requirements, improved information review, and enhanced capabilities. This will include:

(5.1) Developing an operation manual that better defines legal requirements and information sharing between InT elements.

(5.2) Implementing “Enhanced Full Operational Capability” (EFOC) framework standards under which all DoD InT Programs will operate by October 1, 2022.

(5.3) Updating the policy for the appropriate use of PAEI to support analysis of concerning activities within 180 days.

6. Develop and initiate execution of an outreach and education plan related to the InT Program within 90 days.

(6.1) This will include training aids to educate and inform a wide range of audiences regarding the importance of reporting information pertaining to extremist activities and other behaviors of insider-risk concern, as well as what should be reported.

4. CONCLUSION

Extremist activity within the Department of Defense is rare, but even the actions of a few can have an outsized impact on unit cohesion, morale and readiness – and the physical harm some of these activities can engender can undermine the safety of the Total Force. The Department will continue to address insider threats and other activities that might undermine unit cohesion, including extremist activity. These efforts will improve the readiness of our Total Force, ensuring that the United States continues to have the finest, most disciplined military in the world.

REFERENCES

In the course of its review, the CEAWG referenced a wide range of diverse materials to inform its analysis and deliberations. The comprehensive list below includes the primary sources referenced by the working group, most of which are publically available.

10 U.S.C. 1142. (2012). *Preseparation counseling; transmittal of medical records to Department of Veterans Affairs.* Retrieved June 3, 2021, from https://www.govinfo.gov/app/details/USCODE-2006-title10/USCODE-2006-title10-subtitleA-partII-chap58-sec1142

28 C.F.R. Section 0.85. *Definition of Terrorism*. Retrieved on June 3, 2021 from, https://www.law.cornell.edu/cfr/text/28/0.85.

AR 600-20, *Army Command Policy on Extremist Organizations and Activities*.

Case details. *Deborah Morgan v. United States Postal Service*. 798 F.2d 1162 (8th Cir. 1986). Docket: PH07528710588 (1991).

DAPE-MPA. (2021). Applicant Screening Check – Association with an Extremist/Hate Organization or Gang.

Dawson, Jessica. (May 2021). *Cyber Extremism: Extremist Ideologies Targeting the U.S. Military Online.*

Department of Defense. (1996). *The Secretary of the Army's Task Force on Extremist Activities. Defending American Values Report.* Retrieved from the Command and General Staff College Library, Fort Leavenworth, KS.

Department of Defense. (2020). *DoD Report to Armed Services Committees on Screening Individuals who Seek to Enlist in the Armed Forces*.

Department of Defense. (2020). *DoD Report to Congress on Military Personnel and Extremist Ideologies.*

Department of Defense. (2020). *Military Personnel and Extremist Ideologies*.

Department of Defense. (2020). *Stuck in Red Tape: How VA's Regulatory Policies Prevent Bad Paper Veterans from Accessing Critical Benefits*. DoD statement before the House Armed Services Committee. Retrieved on June 4, 2021 from https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=110852.

Department of Defense (2021). *DoD Inspector General's Report to Congress Pursuant to Section 554 of the Fiscal Year 2021 National Defense Authorization Act*.

Department of Defense. (2021). *Review of Services' Implementation of DoDD 5205.16 and DoDI 1325.06*.

Department of Homeland Security Emeritus Center of Excellence, Retrieved June 3, 2021, from https://www.dhs.gov/science-and-technology/centers-excellence.

Department of Veterans Affairs. *Veterans Employment Toolkit. Common Challenges During Re-adjustment to Civilian Life*. Retrieved on June 4, 2021 from https://www.va.gov/VETSINWORKPLACE/challenges.asp.

Defense Personnel and Security Research Center. (2013). *Enhancing the Military Tattoo Screening Process*.

Defense Personnel and Security Research Center. (2005). *Screening for Potential Terrorists in the Enlisted Military Accessions Process*. Retrieved on June 3, 2021, from https://fas.org/irp/eprint/screening.pdf.

DoDD 1304.26. (2016). *Qualification Standards for Enlistment, Appointment, and Induction*.

DoDD 5205.16. (2014). *The DoD Insider Threat Program*.

DoDD 5400.07. (2019). *DoD Freedom of Information Act (FOIA) Program*.

DoDD 5400.11. (2019). *DoD Privacy and Civil Liberties Programs*.

DoDI 1325.06 (2009). *Handling Dissent and Protest Activities Among Members of the Armed Forces.*

DoDI 1332.14. (2019). *Enlisted Administrative Separation.*

DoDI 1332.30. (2019). *Commissioned Officer Administrative Separation*.

DoDI 1400.25, Vol. 731. (2012). *DoD Civilian Personnel Management System: Suitability and Fitness Adjudication for Civilian Employees*.

DoDI 1438.06 (2014). *Workplace Violence Prevention and Response.*

DoDI 5200.02. *DoD Personnel Security Program (PSP).*

DoD Manual 5200.08 Volume 3. *Physical Security Program: Access to DoD Installations*.

DoD SkillBridge Program. Retrieved June 7, 2021, from https://dodskillbridge.usalearning.gov/.

DoD Transition Assistance Program. Retrieved June 7, 2021, from https://www.dodtap.mil/index.html.

Executive Order 9981. (1948). *Desegregation of the Armed Forces*.

Executive Order 11785. (1974). *Relating to Security Requirements for Government Employment, and for Other Purposes*.

Executive Order 13587. (2012). *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*.

Executive Order 13764. (2017). *Amending the Civil Service Rules, EO 13488, and EO 13467 To Modernize the Executive Branch-wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters*.

Flacks, M. and Wiskoff, M. (1998). *Gangs, Extremists Groups, and the Military: Screening for Service*. Security Research Center, Monterey, CA.

Interagency Security Committee. (2019). *Violence in the Federal Workplace: A Guide for Prevention and Response*. Retrieved on June 4, 2021 from https://www.cisa.gov/publication/isc-violence-federal-workplace-guide.

Jones, S., Doxsee, C., Huang, G., and Thompson, J. (2021). *The Military, Police, and the Rise of Terrorism in the United States*. Center for Strategic and International Studies (CSIS) Brief. Retrieved on June 4, 2021 from https://www.csis.org/analysis/military-police-and-rise-terrorism-united-states.

Military One Source. Military Life Cycle: Separation and Transition. Retrieved on June 4, 2021 from https://www.militaryonesource.mil/military-life-cycle/separation-transition/military-separation-retirement/.

NOTAM 21-09, 23 April 2021.Applicant Suitability Check - Association with an Extremist/Hate Organization or Gang.

Owens, R., Evans, J., Foley, J., and Lee, J. (2016). *Countering Violent Extremism – Developing a Research Roadmap: Literature Review*. Retrieved on April 22, 2021 from https://www.dhs.gov/sites/default/files/publications/OPSR_TP_CVE-Developing-Research-Roadmap_Literature-Review_180411-508.pdf.

Profiles of Individual Radicalization in the United States (PIRUS) Data Set. National Consortium for the Study of Terrorism and Responses to Terrorism (START). Retrieved on May 24, 2021 from https://www.start.umd.edu/profiles-individual-radicalization-united-states-pirus-keshif.

Standard Form 86. (2016). Questionnaire for National Security Positions. Retrieved on June 3, 2021, from U.S. Office of Personnel Management https://www.opm.gov/forms/pdf_fill/sf86.pdf.

Stephens, W., Sieckelinck, S., and Boutellier, H. (2021). *Preventing Violent Extremism: A Review of the Literature, Studies in Conflict & Terrorism*. Retrieved on April 22, 2021 from https://www.tandfonline.com/doi/full/10.1080/1057610X.2018.1543144.

Theus Report. (1970). *The Inter-Service Task Force on Education in Race Relations Report and Recommendations*.

Violent Extremism Guide for Army Leaders and Army Security Professionals. Retrieved on May 24, 2021 from https://home.army.mil/jbmhh/application/files/6416/1347/9393/AT_Violent_Extremism_Guide_web.pdf.