Report to the Secretary of Homeland Security Domestic Violent Extremism Internal Review: Observations, Findings, and Recommendations

U.S. Department of Homeland Security
Office of the Chief Security Officer

March 11, 2022

Homeland Security

Contents

Executive Summary

At Secretary Mayorkas' direction, a cross-Departmental working group of senior officials conducted a comprehensive review of how to best prevent, detect, and respond to potential threats related to domestic violent extremism within the Department of Homeland Security (DHS). The Department's Chief Security Officer led the Domestic Violent Extremism Internal Review Working Group (Working Group), which included experts from across the Department, including from DHS oversight offices. The Working Group also consulted with several interagency partners during the course of its review.

The Working Group found very few instances of the DHS workforce having been engaged in domestic violent extremism. However, the Working Group assessed that the Department has significant gaps that have impeded its ability to comprehensively prevent, detect, and respond to potential threats related to domestic violent extremism within DHS. These gaps, which the Department is working with urgency to close, may have impacted DHS officials' ability to adequately identify and address related threats, and include the following:

- a lack of an official definition of "domestic violent extremist," guidance as to what constitutes violent extremist activity, and an established list of behaviors that may be indicators of domestic violent extremism;
- a lack of workforce training specific to identifying and reporting violent extremist activity;
- a lack of specialized training for those best situated to identify violent extremist activity or behaviors that may be indicators of violent extremism (e.g., background investigators, Office for Civil Rights and Civil Liberties inquiry officials, and DHS Insider Threat Program personnel);
- a lack of a centralized, interoperable DHS-wide investigative case management system, as well as standardized reporting and information sharing mechanisms for investigating allegations of violent extremist activity; and,
- insufficient funding needed to support the expansion of the DHS Insider Threat Program, development and implementation of related training programs, establishment of a DHS-wide related reporting mechanism, and implementation of the government-wide federal personnel security reform effort called Trusted Workforce 2.0.

To address these gaps, the Working Group made 15 recommendations described further below to enhance the Department's ability to comprehensively address internal domestic violent extremism-related activity to protect our employees and DHS's ability to continue executing its critical mission.

Background

Every day, more than 250,000 dedicated DHS personnel work to ensure the safety and security of communities across our country. Executing DHS's critical mission requires dedication, honor, integrity, and often, enormous personal sacrifice.

Domestic violent extremism poses one of the most significant terrorism-related threats to the United States. In February 2021, in recognition of the gravity of the threat, Secretary Mayorkas designated for the first time domestic violent extremism as a "National Priority Area" in Federal Emergency Management Agency (FEMA) grant programs, while simultaneously increasing training opportunities for law enforcement partners through domestic violent extremism threat assessment and management programs. Further, DHS has renewed its commitment to sharing timely and actionable information and intelligence with our partners across every level of government, in the private sector, and local communities, as well as with the public. To this end, since January 2021, DHS has issued more than 95 intelligence products related to domestic violent extremism, including five National Terrorism Advisory System (NTAS) Bulletins that highlight the threat posed by domestic violent extremists to the United States and related sources for how to stay safe.

In an April 26, 2021 message to the DHS workforce, Secretary Mayorkas stated that "we must be vigilant in our efforts to identify and combat domestic violent extremism within both the broader community and our own organization." The Secretary further emphasized that violent extremism "has no place at DHS"[1] and directed the Department to "immediately begin a review of how to best prevent, detect, and respond to domestic violent extremism threats within DHS."[2] In response, the Working Group was chartered on May 7, 2021, with the following six objectives:

(1) collaborate with pertinent stakeholders to evaluate and leverage lessons learned, best practices, and previous efforts to define and respond to threats related to domestic violent extremists within DHS;

(2) identify potential gaps in existing responsibilities and authorities;

(3) develop guidance for identifying and responding to violent extremist activity;

(4) identify methods to detect violent extremist activity within DHS;

(5) develop a communication strategy to prevent and combat violent extremist activity through continued training and education of the workforce; and

[1] Secretary Mayorkas Announces Domestic Violent Extremism Review at DHS, April 26, 2021, www.dhs.gov/news/2021/04/26/secretary-mayorkas-announces-domestic-violent-extremism-review-dhs

[2] The Working Group used the definition provided in the Office of the Director of National Intelligence's "Domestic Violent Extremism Poses Heightened Threat in 2021" assessment issued on March 1, 2021, which defines a domestic violent extremist as "an individual based and operating primarily in the United States without direction or inspiration from a foreign terrorist group or other foreign power and who seeks to further political or social goals wholly or in part through unlawful acts of force or violence." It is important to note that the mere advocacy of political or social positions, political activism, use of strong rhetoric, or generalized philosophic embrace of violent tactics does not constitute extremism and is constitutionally protected.

(6) evaluate and identify potential existing departmental resources and capabilities that can be integrated into vetting and ongoing review processes of DHS personnel to detect violent extremist activity.

The Working Group was chartered to conduct a comprehensive review of how best to prevent, detect, and respond to threats related to domestic violent extremism within DHS. There are other policies and practices designed to prevent and respond to harassment based on race, gender, national origin, religion, and other characteristics specifically prohibited by law. Those are not covered by this report. Supervisors and others in leadership positions have additional obligations to avoid speech and conduct that advances extremism or otherwise undercuts the interests of the Department; those are not covered in this report.

Current Domestic Violent Extremism Threat Landscape

A March 2021 unclassified threat assessment prepared by the Office of the Director of National Intelligence (ODNI), Department of Justice, and DHS, noted that domestic violent extremists "who are motivated by a range of ideologies and galvanized by recent political and societal events in the United States pose an elevated threat to the Homeland in 2021."[3] The assessment pointed to newer "sociopolitical developments such as narratives of fraud in the recent general election, the emboldening impact of the violent breach of the U.S. Capitol, conditions related to the COVID-19 pandemic, and conspiracy theories promoting violence" that "will almost certainly spur some [domestic violent extremists] [sic] to try to engage in violence this year."[4]

Violent Extremist Activity in the DHS Workforce

As one of its first tasks, the Working Group conducted a Department-wide data call to assess and analyze the scope of potential threats related to domestic violent extremism across DHS since Fiscal Year (FY) 2019. The data call was hindered by the following factors, which the Department is working to remedy.

First, at the time of the data call, the Department and its Components did not track domestic violent extremism allegations as their own sub-category of misconduct. Instead, such allegations were classified under another sub-category (e.g., workplace violence). Second, the responsibility to investigate allegations regarding violent extremist activity varied across the Department and its Components. Investigations could be led by multiple offices such as the DHS Office of Inspector General, Component offices responsible for internal investigations, or the Component's Insider Threat Program. Further, other gaps that limited our ability to collect and validate data included (1) the lack of an official definition of "domestic violent extremist;" (2) guidance as to what constitutes violent extremist activity, or an established list of behaviors that may be indicators of violent extremism; (3) the lack of a centralized, interoperable DHS-wide investigative case management system; and (4) lack of standardized reporting and information sharing mechanisms for investigating allegations of violent extremist activity.

---

[3] This report was produced as part of President Biden's hundred-day review of U.S. Government efforts to address domestic terrorism. FACT SHEET: National Strategy for Countering Domestic Terrorism https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/15/fact-sheet-national-strategy-for-countering-domestic-terrorism/

[4] Office of the Director of National Intelligence, March 2021. Domestic Violent Extremism Poses Heightened Threat in 2021.

The data call requested coordination by each Component's Insider Threat Official with appropriate lines of effort including: Insider Threat, Human Capital (including Workplace Violence), Internal Investigations, Personnel Security, Counterintelligence, Operations Security, IT Security/Chief Information Security Offices, and other relevant offices. DHS Headquarters and Components were asked to provide anonymized data for the number and results of investigations, insight into how the allegation was initially discovered, the disposition, and other investigative data points. The data call categorized each of the allegations into categories of racially or ethnically motivated domestic violent extremism, animal rights/environmental-related domestic violent extremism, abortion-related domestic violent extremism, anti-government/anti-authority domestic violent extremism, and all other domestic terrorism-related threats.[5]

Initial data call results identified 35 allegations between FY 2019 and the third quarter of FY 2021 characterized as being potentially related to violent extremist activity. Upon further review of the allegations, the working group identified four incidents that involved active participation or support for violent extremist activity over the covered period. The other 31 allegations were either unsubstantiated as being related to domestic violent extremism or found to be miscategorized in the data call responses.

Because of the challenges with identifying, categorizing, and tracking this information, it is possible that the data call resulted in an under-reporting of the number of allegations made and investigations conducted. Future efforts to educate the workforce and provide clear guidance about what constitutes violent extremist activity and how to report it, along with other recommendations in this report, will help ensure that future data calls are more reliable.

Working Group Structure and Methodology

The Working Group included representatives from the Office of the Chief Human Capital Officer (OCHCO), Office of the General Counsel (OGC), Office for Civil Rights and Civil Liberties (CRCL), Office of the Chief Security Officer (OCSO), Office of Strategy, Policy, and Plans (PLCY), Office of Intelligence and Analysis (I&A), Office of Public Affairs, the Privacy Office (PRIV), the Immediate Office of the Under Secretary for Management, and officials who are significantly involved in the employee vetting and review process.

The Working Group established six sub-working groups that were each assigned a corresponding objective to primarily explore and oversee, with each sub-working group similarly composed of representatives from multiple DHS Headquarters offices. The working group held bi-weekly meetings and followed a framework to ensure the development and delivery of a thorough review. It incorporated quantitative and qualitative data from internal and external sources and experts, including:

[5] Office of the Director of National Intelligence, March 2021. Domestic Violent Extremism Poses Heightened Threat in 2021. https://www.dhs.gov/news/2021/03/17/odni-doj-and-dhs-release-unclassified-summary-assessment-domestic-violent-extremism

- analysis of results from the DHS Insider Threat Program data call, review of existing DHS online training modules, and an inventory of current internal and external stakeholder efforts to address domestic violent extremism;
- analysis of over 50 current authorities, directives, instructions, instruction manuals, and policies relating to domestic violent extremism;
- briefing from the DHS Center for Prevention Programs and Partnerships (CP3);
- briefing from the DHS Science & Technology Directorate on insider threats facing domestic law enforcement agencies;
- briefing from the Department of Defense (DOD) Personnel and Security Research Center on the use of Publicly Available Electronic Information (PAEI) in personnel security vetting; and,
- briefings from – and continued partnership with – the Performance Accountability Council (PAC) Program Management Office (PMO), Office of Personnel Management (OPM), and ODNI on the refinement of the guidelines in Security Executive Agent Directive (SEAD)-5, "Collection, Use, and Retention of Publicly Available Social Media Information in Personnel Security Background Investigations and Adjudications," and updates to the various forms used in the background investigation process (e.g., Standard Form 85P and Standard Form 86).

Key Findings and Recommendations

The following 15 recommendations reflect the Working Group's collective findings and represent a combination of short- and long-term opportunities that would enhance the Department's ability to prevent, detect, and respond to violent extremist activity or behaviors that may be indicators of domestic violent extremism. These recommendations are organized around the following five overarching areas: (1) establish baseline policies and guidance; (2) promote employee awareness; (3) enhance methods to identify and address violent extremist activity; (4) foster an integrated approach; and (5) ensure the protection of privacy, civil rights, and civil liberties.

Area 1: Establish Baseline Policies and Guidance

To identify relevant existing resources, expertise, and entities, the Working Group conducted a survey of DHS Headquarters Components to find internal subject matter experts who were leading efforts to identify and address potential threats related to domestic violent extremism, any ongoing participation in related working groups and meetings, and any external partners and stakeholders that could contribute their knowledge on how to address domestic violent extremism threats. Thirteen different DHS entities provided a total of 20 submissions with feedback to this request for information.

The Working Group conducted qualitative content analysis of over 50 current authorities, directives, instructions, instruction manuals, and policies relating to violent extremist activities to aid in assessing potential gaps in existing DHS responsibilities and authorities. As the Working Group undertook its analysis, the need for clearly defined policies and guidance regarding violent extremist activity quickly emerged.

The Working Group analyzed the standards of conduct in place throughout the Department, including identifying elements that could have a bearing on violent extremist activity such as public trust, associations/affiliations, harassment, discrimination, off-duty conduct, retaliation, and election interference. The Working Group discovered that Components' standards of conduct varied in levels of specificity as each addressed employee responsibilities and accepted standards of behavior and ethical conduct tailored to the unique mission set of the respective Component.

It should be noted that the U.S. Coast Guard, the only military organization within DHS, has approximately 48,000 service members who are subject to the Uniform Code of Military Justice. Activities of U.S. Coast Guard Service Members are not covered in this report, as they were separately considered by DOD's countering extremist activity review and are separately covered by the updated DOD Instruction 1325.06, *Handling Protest, Extremist, and Criminal Gang Activities Among Members of the Armed Forces*.

The Working Group found that:

- DHS has not adopted an authoritative definition of "domestic violent extremist" that can be incorporated into policies, guidance, and awareness materials.
- While multiple lists of indicators of domestic violent extremism currently exist throughout the Federal Government, DHS lacks a definitive list of behaviors that may be indicators of domestic violent extremism that can be incorporated into related policies and guidance.
- There is a need for clear policy and guidance regarding what constitutes violent extremist activity for both employees and officials charged with reviewing and addressing potential threats and allegations related to domestic violent extremism. The working group concluded that a directive would be necessary to provide further clarity and guidance on how DHS would identify and respond to violent extremist activity.

Based on the analysis noted above, the Working Group presents the following four recommendations aligned under Area 1.

Recommendation 1: Adopt a consistent definition of "domestic violent extremist" and descriptions of violent extremist activity and integrate both into DHS policies and guidance.

Multiple definitions of domestic violent extremism and violent extremist activity are currently being used by the Federal Government, including by the Federal Bureau of Investigation (FBI), ODNI, and DOD. DHS should use a standard intra-Departmental definition and would be supportive of a process to adopt an interagency-wide definition.

Action 1.1: Adopt a consistent definition of "domestic violent extremist" and clearly define violent extremist activity, so it can be integrated into DHS policies and guidance.

Clarity and consistency as to what constitutes violent extremist activity in the context of DHS employment will help support employee awareness and ongoing efforts to address related activities.

Recommendation 2: Adopt and implement a DHS-approved list of behaviors that may be indicators of domestic violent extremism.

Action 2.1: Adopt an approved list of behaviors that may be indicators of domestic violent extremism, in collaboration with DHS partners and stakeholders, which will best position DHS to prevent, detect, and respond to potential threats related to domestic violent extremism internal to the Department.

The working group developed a proposed list of indicators, in coordination with CRCL, PRIV, OGC, and I&A, and derived in part from those utilized by the FBI and the National Counterterrorism Center (NCTC), that can be used pending further review and approval by DHS.

To develop this list, the working group reviewed existing terrorism indicators found in the current SEADs, the "Homegrown Violent Extremist Mobilization Indicators, 2019 Edition," and additional DHS sources.[6]

The proposed list of indicators was then supplemented with indicators derived from the DHS Anti-Harassment Policy to facilitate the proactive identification of individuals who may pose a domestic violent extremism-related threat.

Recommendation 3: Develop and implement an official DHS Directive that provides guidance on how to identify and respond to violent extremist activity within the Department.

Action 3.1: Develop and implement a DHS Directive that incorporates a consistent definition of "domestic violent extremist," and violent extremist activity, which will standardize guidance across the DHS enterprise on how to identify and respond to violent extremist activity.

The working group drafted a comprehensive DHS Directive, in coordination with several DHS Components, to serve as a foundational document. This Directive will provide further clarity and guidance on how DHS will identify and respond to potential threats related to domestic violent extremism. It is consistent with DHS's terrorism and targeted violence prevention priorities, which focus on preventing acts of violence at the earliest stage possible.

Recommendation 4: Incorporate the list of violent extremist activity into DHS policy.

Action 4.1: Implement a DHS-wide policy on preventing, detecting, and responding to violent extremist activity within DHS.

[6] Joint Counterterrorism Assessment Team, 2019. "Homegrown Violent Extremist Mobilization Indicators, 2019 Edition."

This Department-wide policy would provide guidance on what constitutes violent extremist activity, and remind employees of their oath of office, responsibilities, and obligations as they relate to violent extremist activities.

Area 2: Promote Employee Awareness

The Working Group interviewed subject matter experts and training providers (internal and external to DHS), conducted surveys, and reviewed existing DHS instructor-led in-person and online training courses to identify existing departmental training and education resources that could be leveraged to incorporate topics associated with violent extremist activities.

Using mixed methods of qualitative and quantitative techniques, the Working Group identified 62 courses and 21 books available through DHS learning management systems that may be updated to incorporate domestic violent extremism examples and guidance, and conducted a training needs assessment through interviews, observations, and data calls to validate the requirement.

The Working Group found that:

- DHS currently does not have any specialized training for employees charged with personnel vetting activities on how to identify and adjudicate violent extremist activity;
- DHS lacks an easily accessible online repository of materials specifically related to preventing, detecting, and responding to violent extremist activity, including links to associated directives and guidance, training, and the Employee Assistance Program on the DHS Connect internal website;
- DHS does not have a standardized method to emphasize the importance of reminding employees of their obligations to adhere to established policies, Ethics/Standards of Conduct, their oath of office, reporting requirements, and statutory regulations;
- current DHS training does not include courses that address the threat that domestic violent extremists within the Department could pose to the DHS mission; and,
- any new training should include what constitutes violent extremist activities; the threat it presents to the DHS mission and workforce; and how to identify and report individuals engaged in violent extremist activity.

Based on the analysis noted above, the Working Group presents the following three recommendations aligned under Area 2.

Recommendation 5: Educate the DHS workforce on the threat that domestic violent extremists within the Department could pose to the DHS mission.

Action 5.1: Update current course content offered within DHS learning management systems to incorporate information on how to identify and report potential violent extremist activity. This training would support other efforts that focus on early intervention for employees at risk of engaging in violent extremist activity.

The Working Group proposes updating four courses given the nexus between their current content and identifying and reporting violent extremist activity. These courses include:

- DHS Insider Threat Training
- Violent Extremism Awareness Briefing
- DHS No FEAR Act
- Preventing and Addressing Workplace Harassment

Action 5.2: Pursue and secure additional funding to develop training specific to the identification and reporting of violent extremist activity.

DHS will develop a strategy to secure the resources needed to expeditiously create or update related curricula, including through potential contract vehicles.

Recommendation 6: Inform employees of their obligations to refrain from violent extremist activity and the existing reporting requirements.

DHS employees have a duty to abide by the responsibilities and obligations set forth in their oath of office, Ethics/Standards of Conduct, policies and directives, and agreements entered as a condition of their employment and for access to sensitive information, as well as those outlined in regulatory laws and statutes that are applicable to all citizens.

Action 6.1: Through formal messages from senior leadership and ongoing workforce engagement by leaders at all levels, consistently and clearly inform employees of their obligations to refrain from violent extremist activities. Messaging will also include the protections afforded to employees under the Whistleblower Protection Act, equal employment opportunity laws, and other statutes when engaging with the workforce on what constitutes violent extremist activity.

The Working Group developed the "Domestic Violent Extremism Awareness Discussion Guide for Department Leaders," which will enable and foster communication between leaders and employees and aid in these often-difficult conversations. This Leader Discussion Guide explains the importance and meaning of the oath of office each employee has taken, their responsibility and duty to report, and the Department's expectations of appropriate conduct.
Leadership will be able to reference examples of what is considered protected speech, employee standards of conduct, case studies of violent extremist activity, frequently asked questions, and additional resources and references.

Recommendation 7: Provide training on how to identify and adjudicate violent extremist activity to employees charged with personnel screening and vetting activity.

There are several employee populations, such as background investigators, CRCL inquiry officials, and DHS Insider Threat Program personnel, that will need specialized training to enhance their expertise within their specific discipline.

Action 7.1: Develop and establish a specialized training program for practitioners who are most likely to encounter violent extremist activity and indicators of extremism in the

context of their duties. This will enable them to identify, evaluate, and respond to these threats more effectively.

An important element of this training must be how to engage with individuals who may be displaying early indicators of extremist behavior or may be radicalizing to violence.

Area 3: Enhance Methods to Identify and Address Violent Extremist Activity

The working group distributed a data call to stakeholders who play a primary role in the employee vetting and review process, including OCHCO, OGC, OCSO, CRCL, PLCY, and I&A, to identify existing capabilities and resources that could be integrated into vetting and ongoing review processes of DHS personnel. Specifically, respondents were asked to:

- identify and describe the capability/resource that could be integrated into vetting and ongoing review processes of DHS personnel;
- identify the line(s) of business that manages the capability/resource;
- identify the relationship to the detection, prevention, or response to domestic violent extremism threats;
- identify interdependencies with other resources/capabilities; and,
- identify gaps or limitations on the resource/capability.

The Working Group found that:

- DHS should enhance its existing technical capability to detect and respond to violent extremist activity along the life cycle of an employee.
- DHS does not have a centralized, interoperable DHS-wide investigative case management system that tracks and records employee and contractor misconduct, disciplinary actions, and criminal and administrative investigations. This is an information sharing shortfall for instances specifically where contractors leave a contract prior to the completion of an investigation or inquiry, and the investigation is discontinued due to loss of jurisdiction.
- DHS has varying ways for employees to report violent extremist activity. The lack of a centralized reporting mechanism can be confusing to employees, which may prevent timely reporting and cause delays in routing reported information to the appropriate entity.
- The DHS Insider Threat Program meets the minimum standards specified in Executive Order 13587, but it does not cover all DHS networks.[7] Additional funding is necessary to resource these efforts, as this will greatly enhance the Department's ability to identify and address violent extremist activity and protect from insider threats.

The Working Group also assessed the importance of ensuring that relevant officials are provided with the outcomes of complete, thorough, and timely investigations to take disciplinary action when necessary and as appropriate.

[7] Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," October 7, 2011.

Based on the analysis noted above, the Working Group presents the following seven recommendations aligned under Area 3.

Recommendation 8: Enhance hiring practices through initiatives under Trusted Workforce 2.0 in order to deter and detect individuals engaged in violent extremist activity from applying to work for the Department.

One of the most effective methods of preventing domestic violent extremists from entering the DHS workforce is to discourage individuals engaging in violent extremist activities from applying to the Department in the first place. Clearly articulating the Department's position on violent extremist activity in its recruiting, hiring announcements, and other human capital activity is critical in this regard.

Once a selection is made for a position, background investigations become the primary tool used in the personnel vetting process and are used routinely throughout DHS; however, there are varying levels of implementation based on the sensitivity of the position.[8,9]

Action 8.1: Upon approval by the Office of Management and Budget (OMB), implement changes to Questionnaires for Public Trust and National Security Positions, Standard Form (SF)-85P, Section 27, and the SF-86, Section 29, respectively, which will be designed to yield actionable information that will enhance the detection of violent extremist activity.

Revisions to incorporate additional questions related to violent extremist activities in the various forms used in the background investigation process (e.g., SF-85P and SF-86) are actively being considered by Security and Suitability Executive Agents. Additional enhancements to the background investigation process will be achieved through the larger government-wide personnel security vetting reform effort, Trusted Workforce 2.0.

Action 8.2: Review, in partnership with the Performance Accountability Council (PAC) Program Management Office (PMO), Office of Personnel Management (OPM), and ODNI, the appropriate use of publicly available electronic information (PAEI), including social media, in personnel security vetting and determining eligibility for access to classified information or for holding a sensitive position.

This review will include the feasibility of establishing clearer guidelines in SEAD-5, "Collection, Use, and Retention of Publicly Available Social Media Information in Personnel Security Background Investigations and Adjudications," which enables the use of PAEI, including social media, as part of a personnel security vetting process.

This partnership and continued participation in similar interagency personnel vetting reforms enables the Department to support and inform government-wide efforts to establish clearer

[8] 5 CFR Part 731.106-Designation of Public Trust Positions and Investigative Requirements.

[9] 5 CFR Part 1400.201-Designation of National Security Positions.

guidelines when addressing domestic violent extremism, the use of PAEI, and impacts to the 2008 Joint OPM-ODNI Federal Investigative Standards and adjudicative guidelines.
The OCSO Enterprise Security Operations and Support Directorate has identified and requested, through the Department's Resource Allocation Plan (RAP) process, resource requirements necessary to implement Trusted Workforce 2.0.

Recommendation 9: Establish the intra-departmental sharing capability for investigations and inquiries involving DHS contractors and other non-employee insiders.

Establishing a centralized, interoperable DHS-wide investigative case management system and information sharing procedures for these types of investigations and inquiries will help mitigate against the risk that a contractor under investigation for potential misconduct leaves the applicable contract prior to the completion of the investigation.

Given that DHS has about 170,000 contractors, special consideration must be given to vetting this sizeable population, which has direct authorized access to DHS assets (e.g., facilities, equipment, information, and systems).

DHS has remedies available to address domestic violent extremism threats involving DHS contractors and other non-employee insiders, including limiting or prohibiting access to DHS owned, leased, and operated facilities and/or removing an individual from a contract, as well as referring information to an appropriate criminal investigative agency for further action.

Action 9.1: Establish a working group composed of relevant subject matter experts from across the Department to identify and implement procedures and system capabilities needed to permit information sharing of investigations and inquiries.

Recommendation 10: Promote early intervention to get support to employees who may be at risk of radicalizing to violence.

The benefits of early intervention noted by the Working Group. Several federal departments and agencies have formally established programs designed to deliver peer-based early-stage intervention for employees at risk of radicalizing to violence. DHS should assess these programs as a potential model to replicate internally.
Action 10.1: Develop procedures, leveraging the Center for Prevention Programs and Partnerships (CP3) and OCHCO's existing prevention programs (e.g., employee assistance programs) to provide intervention assistance for DHS employees.

CP3's approach focuses on providing early intervention to help prevent individuals from radicalizing to violence. This approach incorporates violence prevention principles that leverage behavioral threat assessment and management tools and addresses early-risk factors that can lead to radicalization to violence.

DHS should promote and continuously review its existing internal prevention programs (e.g., employee assistance programs) to ensure they are aligned with relevant best practices.

Recommendation 11: Establish efficient and accessible reporting and intake mechanisms to facilitate information sharing among stakeholders charged with addressing allegations of violent extremist activity.

The results of the Department-wide domestic violent extremism data call conducted by the DHS Insider Threat Program demonstrate the importance of having a readily available and easily understood mechanism for employees to report allegations of violent extremist activity, as well as concerns that another DHS employee may be radicalizing to violence, while protecting privacy, civil rights, and civil liberties. Currently, there are multiple ways for employees to report this type of information, including through the DHS OIG hotline, Component-specific hotlines, shared email mailboxes, and website applications. DHS should develop a more standardized process with clear processes and procedures.

Action 11.1: Establish a single reporting platform and intake center for use by employees throughout the Department to streamline and facilitate the intake process to help ensure information is relayed to appropriate entities.

This reporting platform should be designed in coordination OCHCO, OGC, CRCL, and PRIV, and should enable intra-Departmental information sharing with appropriate safeguards.

Action 11.2: Identify resource requirements for establishing a singular, integrated, DHS-wide reporting platform and intake center.

Recommendation 12: Accelerate the expansion of DHS Insider Threat Program capabilities.

The DHS Insider Threat Program continues to expand and enhance capabilities to protect the Department from insider threats, including those related to violent extremist activity. Additional funding is necessary to resource these efforts, as this will greatly enhance the program's ability to identify and address indicators of violent extremist activity.

Action 12.1: DHS should pursue and secure additional funding through appropriations and other means to expand the DHS Insider Threat Program's capability to identify and address violent extremist activity.

The DHS Insider Threat Program should launch an Executive Steering Committee to ensure the program is adequately resourced to carry out its mission. The Committee should also ensure that the program has necessary guidance to meet its objectives.

The DHS Insider Threat Program has identified and requested, through the Department's Fiscal Years 2023-2027 RAP process, the resource requirements necessary to expand its capabilities and will continue to do so for subsequent RAP cycles.

Recommendation 13: Incorporate the DHS list of behaviors that may be indicators of violent extremism into insider threat tools, including user activity monitoring.

Action 13.1: Operationalize the DHS-approved list of behaviors that may be indicators of violent extremism by incorporating these elements into the tools and techniques employed by the DHS Insider Threat Program to enhance the Department's capability to identify and address these threats.

The Working Group drafted a proposed list of these indicators, in coordination with CRCL, PRIV, OGC, and I&A, and derived in part from those developed by the FBI and NCTC, that can be used pending approval by DHS leadership. The DHS Insider Threat Program will use these indicators to enhance capabilities to identify and address threats related to domestic violent extremism.

Recommendation 14: Explore expanding the use of publicly available information, including social media, beyond personnel security vetting, to identify or investigate potential violent extremist activity within the DHS workforce.

Studies and pilots have suggested that certain online activity may represent behavior of potential concern to national security and could be useful in assessing an individual's trustworthiness, judgment, or reliability.[10, 11, 12, 13, 14] PAEI, including social media checks, have proven to be of limited value as stand-alone sources of information. However, when coupled with and corroborated by other data and investigative follow-up, the use of PAEI can be a powerful tool in preventing and detecting domestic violent extremism-related threats.

DHS must continue to examine the use of social media and other PAEI, including within the scope of personnel security vetting, to enhance the Department's security posture in preventing and detecting violent extremist activity.

It is also critical that any study or implementation of social media monitoring is pursued deliberately to protect the privacy, civil rights, and civil liberties of all individuals.

Action 14.1: Host a series of information sharing sessions with DOD, the Intelligence Community, Department of Justice, academia, and industry to identify best practices, frameworks, and adaptation of PAEI, including social media checks, beyond the scope of personnel security vetting to identify and investigate violent extremist activity within the DHS workforce.

[10] PERSEREC-MR-03-Identifying Adjudicatively-Relevent Social Media & Open-Source Content for Personnel Security Investigations, May 2019.

[11] PERSEREC-MR-04-Social Media Business Rule Implementation: Application of Technology for Search, Collection, and Analysis, June 2019.

[12] PERSEREC-MR-05-Standarizing Checks of Publicly Available Electronic Information in the Personnel Security Program, September 2019.

[13] Available Electronic Information and Background Investigations-Lessons Learned from NBIB Social Media Pilot, November 2017.

[14] National Counterintelligence and Security Center-Office of Personnel Management, Department of Homeland Security Publicly Available Electronic Information (PAEI) Pilot, June 2018.

This critical information sharing will include measures to mitigate biases when determining what social media platforms are reviewed and how content is evaluated (e.g., content posted on a given platform is viewed with different scrutiny than similar content on another platform). Therefore, it is critical that any study or implementation of social media collection is pursued deliberately to protect the privacy, civil rights, and civil liberties of all individuals.

Area 4: Foster an Integrated Approach

The Working Group found:

- Subject matter experts from across DHS Components characterized the Working Group as a positive initial step in addressing the potential threat of domestic violent extremism within the workforce and recommended continued intra- and interagency collaboration on related topics through recurring working groups, symposiums, and similar activities.

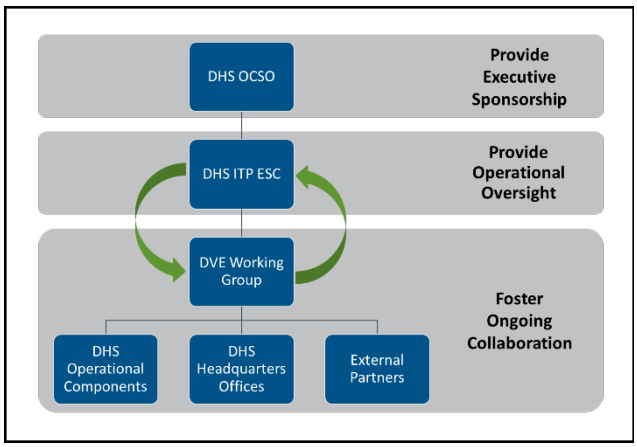
Based on the analysis noted above, the Working Group recommends this action under Area 4.

Recommendation 15: Establish an ongoing DHS Domestic Violent Extremist Working Group.

Successful implementation of these 15 recommendations will require a collaborative cross-functional approach with senior leadership support. The DHS Insider Threat Executive Steering Committee should facilitate the implementation of the final recommendations and coordinate any related actions. This Steering Committee, co-chaired by the Under Secretary for Intelligence and Analysis and the Under Secretary for Management, would serve as a forum for continued discussion on how to enhance the Department's ability to prevent, detect, and respond to threats related to violent extremist activity, including related oversight.

The Steering Committee will also provide a feedback loop to help ensure that any actions taken by the Department to address violent extremist activity achieve intended outcomes, consistent with privacy, civil rights, and civil liberties.
The Working Group also recommends implementing all Trusted Workforce 2.0 requirements, including continuous vetting, as these actions enhance the Department's ability to detect concerning activity within the workforce, to include violent extremist activity.

Proposed Governance Structure



Routine DHS engagements with external partners to include DOD's extremism task force, OMB, academic institutions, and the private sector, will enable collaboration and coordination on the latest research findings, best practices, and sharing of insights to policymakers, other relevant officials, and the DHS workforce.

Action 15.1: The DHS Insider Threat Executive Steering Committee will update the Working Group charter and develop a plan to oversee and monitor the collective efforts of

the working group to share information, identify corrective actions, and implement any changes needed to address violent extremist activity within the Department.

Area 5: Ensure the Protection of Privacy, Civil Rights, and Civil Liberties

All of the Department's efforts to identify and address potential threats related to domestic violent extremism will be closely coordinated with CRCL, PRIV, and OGC to ensure the continued protection of privacy, civil rights, and civil liberties.

Appendix A – Relevant Constitutional, Statutory, and Policy Provisions

The list below includes the primary sources referenced by the Working Group, most of which are publicly available.

- The Constitution of the United States of America
- Title 5, United States Code, Section 3331, "Oath of office"
- Title 5, United States Code, Section 552a, "Records Maintained on Individuals" (Privacy Act of 1974)

Security

- Title 5, Code of Federal Regulations, Part 731, "Suitability"
- Executive Order 13467, "Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information," June 30, 2008
- DHS Directive 110-03, "Review of Unofficial Publications Containing DHS Information," May 17, 2019
- DHS Instruction 262-05-002, "Insider Threat Program," October 1, 2019
- DHS Instruction 262-05-002-01, "Insider Threat Information Sharing Guide," October 11, 2019
- Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," October 7, 2011

General Counsel

- DHS Management Directive 0480.1, "Ethics/Standards of Conduct," March 1, 2003

Human Capital

- DHS Directive 250-09, "Discipline and Adverse Actions Program," November 18, 2016
- DHS Instruction 250-09-001, "Discipline and Adverse Actions Program," July 28, 2018

Civil Rights and Civil Liberties

- Policy Statement 256-06, "Anti-Harassment Policy Statement," April 1, 2019
- DHS Directive 256-01, "Anti-Harassment Program," May 24, 2019
- DHS Instruction 256-01-001, "Anti-Harassment Program," June 7, 2019
- DHS Instruction 256-03-001, "Workplace Violence," October 3, 2016

Intelligence and Analysis

- National Counterterrorism Center, Federal Bureau of Investigation and Department of Homeland Security, "Homegrown Violent Extremist Mobilization Indicators, 2019 Edition"
- Office of the Director of National Intelligence Assessment, "Domestic Violent Extremism Poses Heightened Threat in 2021," March 1, 2021

Security Executive Agent Policies

- Office of the Director of National Intelligence SEAD-1, "Security Executive Agent Authorities and Responsibilities," March 13, 2012

- Office of the Director of National Intelligence SEAD-2, "Use of Polygraph in Support of Personnel Security Determinations for Initial or Continued Eligibility for Access to Classified Information or Eligibility to Hold a Sensitive Position," Revised September 1, 2020
- Office of the Director of National Intelligence SEAD-3, "Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position," June 12, 2017
- Office of the Director of National Intelligence SEAD-4, "National Security Adjudicative Guidelines," June 8, 2017
- Office of the Director of National Intelligence SEAD-5, "Collection, Use, and Retention of Publicly Available Social Media Information in Personnel Security Background Investigations and Adjudications," May 12, 2016
- Office of the Director of National Intelligence SEAD-6, "Continuous Evaluation," January 12, 2018
- Office of the Director of National Intelligence SEAD-7, "Reciprocity of Background Investigations and National Security Adjudications," November 9, 2018
- Office of the Director of National Intelligence SEAD-8, "Temporary Eligibility," May 18, 2020