Scholarship In Practice

Domestic Extremism: How to Counter Threats Posed to Critical Assets

Jessica Baweja[1] [a], Madelyn P. Dunning[1] [b], Christine Noonan[1] [c]

[1] Pacific Northwest National Laboratory

Keywords: domestic extremism, insider threat mitigation, critical asset protection

Counter-Insider Threat Research and Practice

Vol. 1, Issue 1, 2022

Although facilities with sensitive information, hazardous materials, critical infrastructure, or other sensitive items have security measures in place to protect their assets, the threat of domestic extremism (DE) has challenged those security measures in new ways. The project described in this paper used focus groups to identify best practices, tools, or techniques relevant to preventing or countering DE and sought to identify gaps in security measures. Five focus groups were conducted to understand how to protect critical assets against the threat of DE presented by radicalized insiders who might seek to harm the organization. Results underscore the importance of organizational culture, codes of conduct, and behavior observation programs in prevention of DE events. In addition, results emphasized the value of multidisciplinary teams, employee assistance programs, and regular threat assessment as resources when responding to DE incidents. However, monitoring of social media and lack of adequate resources remain challenges when attempting to prevent or counter the DE threat. This paper aims to extend current knowledge regarding effective prevention and response measures to mitigate DE threats within organizations managing hazardous materials (e.g., chemicals or radioactive material). Recommendations regarding best practices for insider threat mitigation programs specific to DE are provided.

Domestic extremism (DE) is an area of increasing concern for the United States and its allies, as highlighted in recent analyses by the Office of the Director of National Intelligence (ODNI, 2021). Although there has been debate regarding the specific definition of DE, for the purposes of this paper, DE is defined as a belief system that exists outside of more broadly accepted societal belief systems, generally because the tactics or ideas are objectionable and involve radical change to society, government, or religion (Anti-Defamation League, n.d.; Rose et al., 2020). DE pre-

[a] Jessica Baweja is a social scientist at Pacific Northwest National Laboratory (PNNL) where she supports research and operations in insider threat and personnel security, including extremism, mis- and dis-information, and trustworthiness and reliability assessments. She has conducted a variety of research projects exploring psychological indicators of insider threat, evaluating the utility of alternative data sources for personnel vetting, and has developed training materials for use in insider threat operations. She has experience using both quantitative and qualitative research methods, with an emphasis on survey design and analysis and experimental design, semi-structured interviewing, content analysis, and secondary data analysis. Prior to joining PNNL, she spent six years as a behavioral research scientist and manager for Northrop Grumman in personnel security and insider threat research supporting the U.S. Dept. of Defense Personnel and Security Research Center (PERSEREC). She holds a Ph.D. in social-personality psychology and a master's degree in experimental psychology.

[b] Ms. Dunning is a social scientist at Pacific Northwest National Laboratory (PNNL) where she applies computational social science methods and techniques in support of the national security and policy communities. She has experience in insider threat mitigation and personnel risk assessment, social network analysis, red teaming, manual and automated content analysis, and graph modeling of CBRNE terrorism and crime scenarios, supporting projects with a variety of U.S. government agencies. Prior to joining PNNL, Ms. Dunning supported the Center for Intelligence Research Analysis and Training at Mercyhurst University. She received her master's degree in Applied Intelligence from Mercyhurst University. Ms. Dunning also holds a bachelor's degree in Russian with a minor in Law and Justice from Central Washington University, for which she studied abroad in Moscow, Russia.

[c] Christine Noonan is an applied social scientist and program manager at Pacific Northwest National Laboratory. Originally trained as a cultural anthropologist, she has been researching, publishing, and presenting on insider risk and threat mitigation within critical infrastructure sectors for more than a decade. She currently leads a diverse group of research staff focused on the protection of nuclear materials and facilities worldwide. The program partners with countries and international organizations to promote global nuclear security norms and standards; builds and sustains capabilities to prevent theft, sabotage, and illicit use of weapons-usable nuclear materials; and investigates emerging security threats, risks, and mitigation strategies. She received a doctorate in Law and Policy from Northeastern University. Dr. Noonan is a certified Project Management Professional, a Certified Counter-Insider Threat Professional, an active member of the Association of Threat Assessment Professionals and serves as Associate Editor for the journal *Counter-Insider Threat Research and Practice*.

sents a threat to organizations due to potential risks posed by trusted insiders who might enter or become radicalized and seek to do harm (Federal Bureau of Investigation, 2020; Wolfowicz et al., 2020). The focus of this paper, therefore, is on the threat of insiders radicalized by DE beliefs who may commit acts of sabotage, violence, or theft of sensitive information in the name of those beliefs.

For facilities that protect sensitive information, hazardous (e.g., radiological) materials or critical infrastructure, the threat of DE is particularly grave. Due to the potential for mass destruction, critical infrastructure—including those containing chemical, biological, radiological, nuclear, and explosive (CBRNE) materials—present attractive targets to domestic extremists (Fleer, 2020). Although there is little evidence of terrorist groups targeting facilities with CBRNE materials, there are indications that far-right extremists have pursued such materials for use in potential weapons for their attacks (Brill & Bernhard, 2020; Fleer, 2020). More broadly, despite the lack of information on successful attacks (or failed plots) against critical assets, domestic extremists believe threat-making towards US critical infrastructure is an effective mechanism to create chaos and advance their ideological goals (DHS, 2022b). Radicalized insiders present an elevated risk due to their access. Therefore, it is imperative that security programs at such facilities have measures in place to address threats posed by DE.

To better understand how organizations articulate and are prepared to effectively counter the threat, we conducted a series of focus groups with two complementary goals: (a) identification of best practices, tools, or techniques relevant to preventing or countering DE; and (b) subject matter expert elicitation of potential gaps in security measures that may need to be corrected or enhanced.

Method

To meet these objectives, in the summer of 2021, five focus group sessions were conducted with twenty-two subject matter experts (SMEs) in critical asset security. SMEs answered questions focused on best practices, recent trends in DE, and finally, security program initiatives. A more complete description of the methods employed in this study may be found in Baweja et al. (2021). The primary method of data collection was focus group sessions with SMEs in critical asset security. SMEs in critical asset security were identified through their association with professional organizations focused on security and in some cases, via the personal or professional networks of the research team members. Participants included academic researchers, security professionals at organizations with critical assets (e.g., radiological material), and insider threat professionals within the US Federal Government. Five focus group sessions were conducted via videoconference, each 90 minutes in length. The number of participants ranged between three and seven per focus group.

Focus group questions were structured to elicit SME input to understand the definition of DE, trends, or changes in the threat of DE, security measures or best practices important for countering the threat, and finally, to identify gaps in security measures. A list of exemplar questions is shown in Table 1. Although the questions were generally consistent, the exact nature of the phrasing or order was occasionally altered depending on the flow of the discussion.

During the focus groups, notes were taken to capture the main points discussed. After the focus groups were completed, a thematic analysis was conducted to identify, organize, and summarize the themes from the conversations (Braun & Clark, 2012). Three team members independently reviewed the notes and created codes to describe the patterns that they identified; then, they created themes to capture those patterns. The team members then met to reach consensus regarding the themes extracted and revised them to clarify any key points expressed by the SMEs during the focus group discussions.

Results

Thematic analysis of the focus group notes produced seven themes related to countering DE, summarized in Table 2. Focus group participants recognized the evolving nature of the DE threat which is exacerbated by the current sociopolitical environment in the US. Further complicating matters is inconsistency or lack of clarity in definitions of what constitutes DE in thought versus expressed behavior and threat activity. To address these challenges, threat assessment and mitigation must be collaborative and encourage information sharing while simultaneously protecting individual civil liberties. Additionally, human-centric security measures and organizational leadership are viewed as vital to effectively counter the threat.

The seven themes underscored several best practices which can be rolled-up into two primary categories: prevention, and response. Preventive measures are designed to minimize the potential of a domestic extremist threat to occur; response measures are implemented after a potential threat has been identified. Below, we describe the findings of the study relating to the major concerns of *Prevention* and *Response*. We provide representative comments (paraphrased for clarity, brevity, and to preserve anonymity) to emphasize the main ideas

Prevention

SMEs highlighted the importance of a strong organizational culture, implementation of codes of conduct, and behavior observation programs as key preventive security measures against DE threats.

Organizational Culture. SMEs emphasized the importance of fostering a strong organizational culture to effectively prevent domestic extremist threats. Specifically, they discussed the importance of a caretaker culture, where organizations focus on making people feel comfortable coming forward about concerning behaviors or stressors. Organizations can do this by emphasizing that concerns will be addressed appropriately, and when possible, they will provide support rather than take more punitive measures (e.g., termination).

> *One of the biggest gaps is the absence of robust culture. Not necessarily security culture, but caretaker culture. The employee is an investment and an asset, not just a potential threat.*

Table 1. Focus Group Questions

Category	Exemplar Questions
Comprehending the Threat	• What terminology is used to refer to individuals espousing domestic extremist ideology (e.g., domestic extremism, domestic violent extremism, racially or ethnically motivated violent extremism)? • Does organizational policy define terminology used to describe the threat? • How does your organization learn about potential DE threats? • Are good practices and lessons learned shared with others?
Understanding Current State	• How are DE threats to critical asset security characterized? • What primary security measures are used to protect critical assets from DE attacks? • What tools are especially helpful for protecting against DE threats?
Moving Towards Future State	• Are there new or changing threats to critical assets? • How do evolving threats impact security measures? • Which security measures are crucial to reduce DE threats? • What gaps in tools, technology, or security management (including policy) need to be addressed to more effectively counter DE threats?

Table 2. Focus Group Themes

Theme	Description
Culture	SMEs stressed that the focus of insider threat programs should emphasize wellness and early intervention as a part of a supportive culture to help reduce the potential threat of DE.
Privacy	Because DE can relate to individual opinions or beliefs, which may or may not relate to a concrete threat, SMEs emphasized the importance of protecting privacy, civil rights, and civil liberties when working to secure facilities, assets, and materials.
Sociopolitical Environment	The current sociopolitical environment in the US, such as the polarized nature of political discourse, has increased the potential threat of DE.
Definitions	Confusion remains regarding the definitions of DE, creating challenges for enforcement.
Dynamic Threat	The threat of DE is continually changing, and organizations need to remain informed through regular threat assessment.
Human Security	A strong focus on the human aspect of security through personnel training, a robust security culture, and an emphasis on reporting of security concerns was emphasized as important for protecting against the threat of DE.
Collaboration	Because the domestic extremist threat can cross organizational and international boundaries, communication and collaboration are important to better understand the threat and to develop best practices across organizations.

By accentuating the importance of wellness, support, and early intervention, organizations can increase the likelihood that concerns will be reported before they escalate to a potentially damaging incident. Other recent publications in the US also discuss the importance of a culture of reporting and prevention in the mitigation of insider threat (Cybersecurity and Infrastructure Security Agency, 2020), listing a protective and supportive culture as a core principle in insider threat mitigation.

Code of Conduct. A code of conduct is important for organizations to develop and maintain so that all employees understand what is and is not permissible behavior in their workplace. Generally, the SMEs talked about ensuring that employees are civil in the workplace and aware of appropriate conduct, especially as it relates to potentially sensitive areas, such as personal, social, or political beliefs.

> *Organizations need to go back and get a code of conduct. If they have one, review it, and talk about civility in the workplace.*

As one example, the Department of Defense published new guidance defining prohibited extremist activities for US military service members as part of a department-wide effort to address extremism in the ranks (DoD, 2021). This represents a strong example of precisely defining prohibited conduct to clarify what is and is not permissible behavior in the workplace.

Behavior Observation Programs. SMEs emphasized the importance of human intelligence in preventing domestic extremist threats—that is, ensuring that employees are connecting with each other and their supervisors regularly to observe any unusual behavior or changes in behavior. This is also highlighted by programs such as the Department of Homeland Security's "See Something, Say Something" initiative, where people are encouraged to report on suspicious behavior they observe (DHS, n.d.).

> *If our supervisors had regular one-on-ones with employees, we would gather a lot more information than we do now. We see in struggling organizations they are not connecting regularly with their employees, and this gives you the ability to detect changes in behavior.*

A well-rounded human reliability program is a useful tool for DE prevention, as it encourages individuals to identify unusual behaviors that may be indicative of insider radicalization. However, SMEs did recognize that it can be challenging to identify whether a specific behavior might be considered unusual or suspicious, particularly if context for the individual (i.e., their usual patterns of behavior) is lacking.

SMEs also suggested that pre-employment screening and vetting processes (e.g., background checks of criminal and financial behaviors) may be useful for DE prevention efforts. More broadly, recent guidance has suggested a human reliability program, including initial background investigations, continuous evaluation for individuals with privileged access, and robust closeout procedures if an employee is terminated might be an important part of DE prevention efforts (CISA, 2020; World Institute for Nuclear Security (WINS), 2020).

Response

When responding to threats of DE within their organizations, SMEs emphasized that organizations should leverage a multidisciplinary team, offer employee assistance programs, and conduct regular threat assessments to ensure that their response measures are effective against a dynamic threat.

Multidisciplinary Teams. Multidisciplinary teams are key to properly responding to potential domestic extremist threats and to insider threat mitigation programs more generally (DHS, 2019; Ellis et al., 2020; National Insider Threat Task Force, 2017). Not only are these teams important to information-sharing, but different groups have different areas of knowledge and expertise that might be helpful when creating an appropriate response for a specific case.

> *How do you thread that needle, have that discussion about extremism, build a culture within an organization that tolerates potentially extreme opinions but keeps them out of the workplace? It is multidisciplinary; it involves line leaders, HR, and others.*

As DHS terrorism prevention guidance highlights, intervention and threat management is an inherently multidisciplinary activity that requires inputs from law enforcement, human resources, mental health, and security professionals from across an organization to ensure that best practices are applied (DHS, 2019).

Employee Assistance Programs. In addition, SMEs highlighted that organizations should strive to provide resources to individuals who are a potential domestic extremist threat, such as mental health resources or financial support, as suggested by terrorism prevention resources (DHS, 2019).

> *No one wants to turn in their friend who they're concerned about, because it could end their career. We need to rebrand. We are not trying to turn someone in, we are trying to turn them around by getting them assistance early before they have done anything bad.*

In one example of this approach to threat mitigation, the Defense Security Service (DSS) and the Center for Development of Security Excellence (CDSE) published a series of videos entitled, "Turning People Around, Not Turning Them In" (DSS and CDSE 2019) that emphasized early intervention as the priority of insider threat mitigation programs. Programs for financial or mental health counseling can help employees to address stressors in a constructive way, reducing the likelihood that they will use violent means to resolve their problems (DHS, 2019).

Threat Assessment. SMEs underscored the need for organizations to remain informed and prepared to address a changing and growing threat environment.

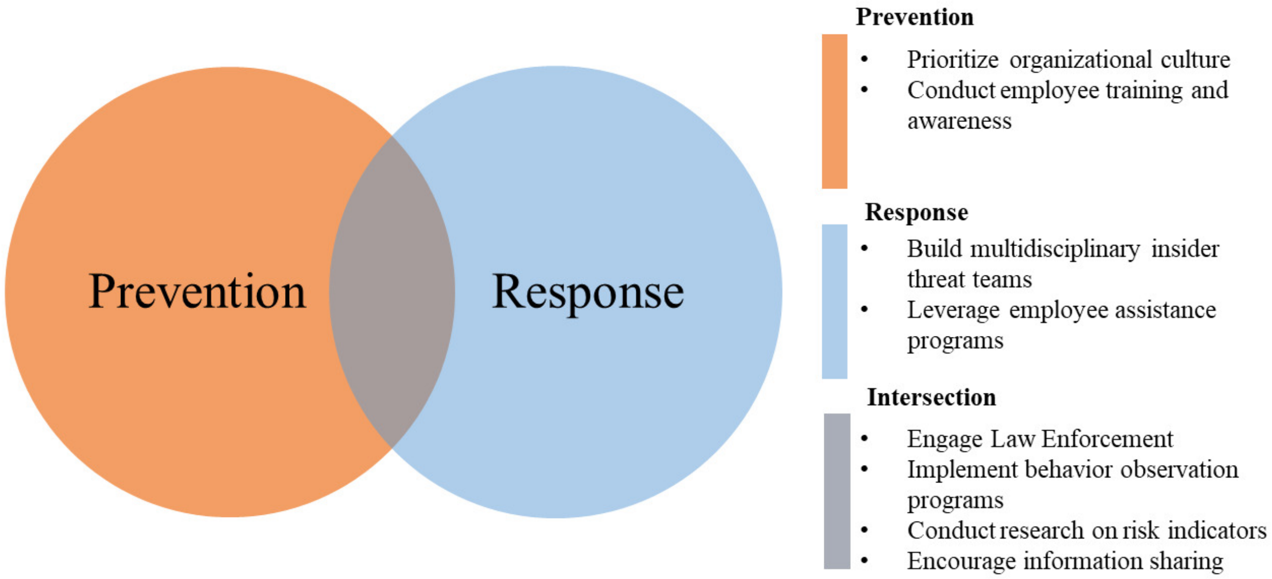
> *The threat is not as easily categorized as before. What might seem to be a local or traditional domestic threat may be a foreign influence campaign. How can we stay on top of the rapidly changing threat posture?*

The US Federal Government has responded to DE by warning agencies and law enforcement partners to be vigilant against the growing threat (DHS, 2022b). Conducting regular assessments of the threat is critical to ensure that any response measures in place are effective against potential DE threats.

Potential Gaps in Security Measures

There were two areas of potential concern or gaps in security: social media monitoring and lack of resources. There is increasing evidence that social media plays an important role in radicalization processes (DHS, 2019; ODNI, 2021; White House, 2021). Monitoring of employees' social media activity might therefore provide indicators or warnings that an individual is at risk of radicalization to extremism and potential violence. However, there are substantial legal and privacy concerns regarding the use of social media for vetting and monitoring purposes (see, e.g., Ghoshray, 2013). Thus, although the lack of social media monitoring was discussed as a potential gap, SMEs also acknowledged that these privacy and legal concerns would need to be addressed before organizations are able to effectively implement a social media monitoring program. Likewise, the DHS Domestic Violent Extremism Internal Review Working Group also recommends expanding the use of social media to identify domestic violent extremism activity within DHS, while recognizing the need to monitor deliberately to protect privacy and civil liberties (DHS, 2022a).

Findings also emphasized that, to effectively prevent domestic extremist threats from manifesting in action, organizations and the federal government need to prioritize the threat in policy and allocate resources accordingly. These findings echo those of DHS' Domestic Violent Extremism Internal Review Working Group, which argues that expansion of the DHS Insider Threat program is insufficiently funded (DHS, 2022a). There is evidence that the US Federal Government has prioritized DE, particularly in the wake of the events at the Capitol Building on January 6, 2021, as highlighted in the recent national strategy to counter domestic terrorism (2021; White House, 2012). In another example, DoD held a department-wide stand-down in April 2021 to address and discuss extremism in the ranks and solicit service members' and civilians' input on the issues (Secretary of Defense, 2021), and subsequently revised guidance to service members regarding prohibited activities (DoD, 2021). Following these examples, organizations with critical assets should work to ensure that their insider threat mitigation programs, human resources, and training personnel have the time, tools, and financial resources to accomplish the task of addressing DE.



Prevention

- Prioritize organizational culture
- Conduct employee training and awareness

Response

- Build multidisciplinary insider threat teams
- Leverage employee assistance programs

Intersection

- Engage Law Enforcement
- Implement behavior observation programs
- Conduct research on risk indicators
- Encourage information sharing

Figure 1. Recommendations for Preventing and Countering DE

Conclusions and Recommendations

This paper describes the core themes identified during a series of focus groups with SMEs in critical asset security. Specifically, the focus group findings highlight the prevention and response measures SMEs identified as most important to address the potential insider threat posed by DE. Recommendations are provided for organizations to inform the prioritization of enhanced security measures.

Many of the practices identified and presented herein are widely acknowledged as key components to an effective insider threat mitigation program. However, the results identify specific practices that might be especially important to counter the threat posed by DE. Security measures such as organizational culture, behavior observation programs, and codes of conduct may bolster preventive measures to mitigate threats posed by radicalized insiders. Additionally, recent counterextremism and counterterrorism publications highlight the impact strong social connections (e.g., regular employment, strong relationships with friends and family) have on individuals, making them less likely to succumb to extreme ideologies (DHS, 2019; National Security Council, 2021; White House, 2021). Overall, these findings suggest that organizations should foster strong security cultures, provide clear guidance for employee behavior, and consider creation of behavior observation programs (as legally authorized and appropriate) to address early intervention for insiders potentially vulnerable to radicalization or other DE related concerns.

Recommendations

While the following recommendations apply generally to insider threat mitigation practices, we have included specific recommendations from SMEs that can help prioritize or re-prioritize insider threat mitigation resources that address potential domestic extremist threats. Figure 1 presents a summary of the recommendations.

- Organizations should prioritize culture as a critical factor in preventing DE incidents. In addition to the code of conduct, suggestions include a self-assessment of security culture (see Sas et al., 2021 for a review of existing tools to assess security culture) and subsequent action plan, security education and training for personnel, and promotional products and training aids to support that training. Early intervention and well-being should be prioritized whenever possible to encourage employee reporting of anomalous or suspicious behavior and promote employee wellness.
- Employees in critical positions (e.g., with access to sensitive information or hazardous materials) should receive training in insider threat mitigation and behavior observation including behaviors indicative of motivation, preparation, or mobilization towards extremist behavior (National Counterterrorism Center, 2021). Many of those behaviors are indicative of other insider threat concerns, such as social isolation, absenteeism, or attempts to test security (see WINS, 2020 for other specific suggestions).
- A multidisciplinary team is an important attribute of an effective insider threat mitigation program (CISA, 2020). Diverse subject matter expertise provides opportunity to address and respond to security concerns using a variety of different approaches and methodologies with a common goal (Ellis et al., 2020). Organizations can refer to guidance from the National Insider Threat Task Force (2017) to ensure that their insider threat mitigation programs draw from expertise across the organization to respond to DE threats most effectively.
- Employee assistance programs serve an essential role in positive organizational response to potential insider threat concerns. Resources provided, such as counseling or referrals, could help to mitigate per-

sonal grievances or stressors before they escalate into counterproductive workplace behaviors, an incident related to DE or insider threat more generally. Organizations should invest in these programs as a potential de-escalation tactic in cases of potential DE concern.
- Given the rapidly changing threat environment identified by SMEs, organizations should engage with law enforcement, stakeholders, and other partner organizations (e.g., organizations with similar assets) to remain apprised of real or perceived DE threats.
- Although not highlighted in the focus groups, results highlight a lack of data on DE for research and analysis (e.g., Mulligan et al., 2021). The US Federal Government would benefit by continued work with researchers to collaborate and share data, where possible. Increased knowledge regarding the indicators of DE or radicalization will enable better identification and development of effective preventive or mitigation measures. As possible, this will facilitate more robust, generalized knowledge of behavioral precursors and of DE in general, providing organizations with critical assets more information on how best to secure those assets and their workforce.

These recommendations clearly articulate the benefits of investing in prevention and response measures focused on DE. By doing so, organizations can be proactive in supporting employees in a manner that addresses concerning behavior, potential grievances, and interpersonal stressors through a variety of strategies.

This research solicited insights from SMEs with experience in critical asset security, specifically, measures which may prove valuable for preventing or responding to DE threats. This preliminary qualitative research provides valuable insights. Additional research is needed to validate these findings. For instance, a quantitative survey conducted among a broader community of security professionals would help support additional investments into administrative and technical measures best suited to address DE.

In addition, insider threat mitigation efforts should be informed by recent guidance from relevant organizations, such as the DHS terrorism prevention resources (2019), CISA's insider threat mitigation guide (2020), and the recent best practices guide in countering violent extremism issued by WINS (2020). By strengthening human-centric security measures, organizations can mitigate potential threats posed by radicalized insiders.

Acknowledgments

This paper presents a summary of the key results of the focus groups. See Baweja et al. (2021) for a literature review on DE and additional detail on the focus group results. The authors express appreciation to the US Department of Energy, National Nuclear Security Administration, Office of Radiological Security for their support of this work. Pacific Northwest National Laboratory (PNNL) is operated by Battelle Memorial Institute for the US Department of Energy under contract DE-AC05-76RL01830. The research plan for the work discussed in this paper was reviewed by the Pacific Northwest National Laboratory Human Research Protection Program Manager and was determined to be 'not human subjects' research.'

Submitted: January 28, 2022 PDT, Accepted: May 17, 2022 PDT

References

Anti-Defamation League (ADL). (n.d.). *Defining extremism: A glossary of white supremacist terms, movements and philosophies*. Retrieved May 20, 2021, from https://www.adl.org/education/resources/glossary-terms/defining-extremism-white-supremacy

Baweja, J. A., Dunning, M. P., Ackerman, C. M., & Noonan, C. F. (2021). *Domestic extremism: Countering the threat posed to critical assets*. Pacific Northwest National Laboratory.

Braun, V., & Clark, V. (2012). Thematic analysis. In H. Cooper, P. M. Camic, D. L. Long, A. T. Panter, D. Rindskopf, & K. J. Sher (Eds.), *APA Handbook of Research Methods in Psychology, Vol. 2: Research Designs: Quantitative, Qualitative, Neuropsychological, and Biological* (pp. 57–71). American Psychological Association.

Brill, K. C., & Bernhard, J. H. (2020). Preventing the preventable: Strengthening international controls to thwart radiological terrorism. *Bulletin of the Atomic Scientists*, *76*(4), 206–209. https://doi.org/10.1080/00963402.2020.1778371

Cybersecurity and Infrastructure Security Agency. (2020). *Insider threat mitigation guide*. https://www.cisa.gov/sites/default/files/publications/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf

Defense Security Service and the Center for Development of Security Excellence. (2019, January 3). *Episode 4: Meeting of the minds*. https://www.youtube.com/watch?v=RZHQW3d819M

Department of Defense. (2021). *Handling dissident and protest activities among members of the armed forces, incorporating change 2, effective December 20, 2021* (DoD Instruction 1325.06). https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/132506p.PDF

Department of Homeland Security. (n.d.). *If you see something, say something®*. Retrieved January 24, 2022, from https://www.dhs.gov/see-something-say-something

Department of Homeland Security. (2019). *Strategic framework for countering terrorism and targeted violence*. https://www.dhs.gov/sites/default/files/publications/19_0920_plcy_strategic-framework-countering-terrorism-targeted-violence.pdf

Department of Homeland Security. (2022a). *Report to the Secretary of Homeland Security domestic violent extremism internal review: Observations, findings, and recommendations*. https://www.dhs.gov/publication/dhs-report-domestic-violent-extremism-internal-review

Department of Homeland Security. (2022b, February 7). *National terrorism advisory system bulletin*. https://www.dhs.gov/sites/default/files/ntas/alerts/22_0207_ntas-bulletin.pdf

Ellis, B. H., Miller, A. B., Schouten, R., Agalab, N. Y., & Abdi, S. M. (2020). The challenge and promise of a multidisciplinary team response to the problem of violent radicalization. *Terrorism and Political Violence*, 1–18. https://doi.org/10.1080/09546553.2020.1777988

Federal Bureau of Investigation. (2020). *Domestic terrorism: Definitions, terminology, and methodology*. https://www.fbi.gov/file-repository/fbi-dhs-domestic-terrorism-definitions-terminology-methodology.pdf

Fleer, B. K. (2020). Radiological-weapons threats: Case studies from the extreme right. *The Nonproliferation Review*, *27*(1–3), 225–242. https://doi.org/10.1080/10736700.2020.1775987

Ghoshray, S. (2013). The emerging reality of social media: Erosion of individual privacy through cyber-vetting and law's inability to catch up. *The John Marshall Review of Intellectual Property Law*, *12*(2), 551–582.

Mulligan, K., Steele, B., Clark, S., Padmanabhan, A., & Hunkler, R. (2021). *A national policy blueprint to end white supremacist violence*. Center for American Progress and the McCain Institute for National Leadership. https://www.americanprogress.org/article/national-policy-blueprint-end-white-supremacist-violence/

National Counterterrorism Center. (2021). *US violent extremist mobilization indicators, 2021 Edition*. https://www.dni.gov/files/NCTC/documents/news_documents/Mobilization_Indicators_Booklet_2021.pdf

National Insider Threat Task Force. (2017). *Insider threat guide: A compendium of best practices to accompany the national insider threat minimum standards*. https://www.dni.gov/files/NCSC/documents/nittf/NITTF-Insider-Threat-Guide-2017.pdf

National Security Council. (2021). *National strategy for countering domestic terrorism*. https://www.whitehouse.gov/wp-content/uploads/2021/06/National-Strategy-for-Countering-Domestic-Terrorism.pdf

Office of the Director of National Intelligence. (2021, March 1). *Domestic violent extremism poses heightened threat in 2021*. https://www.dni.gov/files/ODNI/documents/assessments/UnclassSummaryofDVEAssessment-17MAR21.pdf

Rose, A. E., Prina, D. P., Palmer, M. D., & Rapoza, B. (2020). *Leveraging FBI resources to enhance military accession screening and personnel security vetting*. Defense Personnel and Security Research Center.

Sas, M., Hardyns, W., van Nunen, K., Reniers, G., & Ponnet, K. (2021). Measuring the security culture in organizations: A systematic assessment of existing tools. *Security Journal*, *34*(2), 340–357. https://doi.org/10.1057/s41284-020-00228-4

Secretary of Defense. (2021). *Stand-down to address extremisms in the ranks. Memorandum for Senior Pentagon Leadership, Defense Agency and DoD Field Activity Directors*. https://media.defense.gov/2021/Feb/05/2002577485/-1/-1/0/STAND-DOWN-TO-ADDRESS-EXTREMISM-IN-THE-RANKS.PDF

The White House. (2012). *Presidential Memorandum -- National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*.

The White House. (2021). *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/

Wolfowicz, M., Litmanovitz, Y., Weisburd, D., & Hasisi, B. (2020). What is the state of the quantitative literature on risk factors for radicalization and recruitment to terrorism? In D. Weisburd, E. Savona, B. Hasisi, & F. Calderoni (Eds.), *Understanding Recruitment to Organized Crime and Terrorism* (pp. 25–53). https://doi.org/10.1007/978-3-030-36639-1_2

World Institute for Nuclear Security (WINS). (2020). *Countering violent extremism and insider threats in the nuclear sector.* (Version 2.0).