Protecting the U.S. Government from Far-Right Insider Threats

By Daryl Johnson and Alejandro J. Beutel

Contents

Executive Summary ........................................... 3
Policy Recommendations .................................... 3

Introduction ..................................................... 5
Background ..................................................... 5

Defining the Scope and Key Terms/Concepts of this Report ............... 6
Scope ............................................................. 6
"Insider" and "Insider Threat" .................................. 6

Overview of Personnel Vetting Processes ........................... 8

Manifestations of Insider Threats and Their Link to Far-Right Extremists ............... 9
Activities of Far-Right Extremists with Public Trust/Security Clearance Positions ............... 9
Anti-government Extremists ..................................... 10
Militia Extremists ................................................. 11
White Supremacists/Nationalists .................................. 11
Other Far-Right Actors and Beliefs ................................ 12

Policy Recommendations ....................................... 13
Steps Taken, Steps Ahead ....................................... 15

Endnotes ............................................................ 18

The content and views expressed in this intelligence briefing are those of the authors and should not be taken to reflect an official policy or position of the New Lines Institute for Strategy and Policy.
Executive Summary

The U.S. federal government (USG) employs hundreds of thousands of people who hold positions of trust, including ones requiring security clearances. It is imperative that those assessing, investigating, and adjudicating government personnel background checks and security clearances have knowledge and interest in ensuring that malicious actors, irrespective of their underlying motives, are prevented from joining this trusted workforce.

This policy report will discuss individuals in USG employment, including those with security clearances, who have ties to far-right extremist movements and activities. The report focuses on far-right actors who potentially pose insider threats due to their sizeable support base and their history within the federal security-related workforce. In particular, the authors surveyed publicly reported insider threat activities of white supremacists/nationalists, anti-government extremists, militia extremists, and other far-rightists.

To the extent that far-rightists are publicly discussed in association with insider threats, it is typically in terms of terrorism and other forms of political violence aiming to unlawfully overthrow the USG or coerce it into meeting extremists’ ideological objectives. While this characterization is not inaccurate, it is only one aspect of insider threats far-right actors potentially
pose. Consistent with the full spectrum of insider threats posed by actors of various motivations, far-right insider threats manifest in kinetic (i.e., violent) and non-kinetic ways. Non-kinetic threats include operational security, information security, harassment/equal employment opportunity, and reputational risks to the USG and its workers.

**Policy Recommendations**

We offer the following recommendations to policymakers in government to mitigate the risk of insider threats motivated by far-right ideologies promoting extremism, hate, and violence:

First, the U.S. Intelligence Community must revisit and, if needed, revise strategies to deal with operational security concerns related to extremists employed throughout the entire USG enterprise.

Second, security professionals involved in government security vetting processes need basic, as well as advanced, training related to far-right extremism.

Third, government entities responsible for investigating, adjudicating, maintaining, and updating government clearances for both government employees and contractors should:

- Revise clearance questionnaires to capture applicant responses related to extremist participation beyond terrorist organizations or subversive groups wanting to overthrow the government by force or violence.
- Clarify and institute policies to enable background investigators and other security officials to access publicly available information that could identify extremist affiliations and activities of concern, per FBI/DHS (Department of Homeland Security) and other relevant agency training.
- Ensure that continuous evaluation programs and other vetting initiatives identify new information regarding trusted employees’ extremist affiliations and activities of concern, per FBI/DHS and other relevant agency training.

Fourth, USG entities involved in vetting processes should consider making an employee’s participation in, affiliation with, or support for extremist groups/movements/causes that advocate violence against USG officials or property a reportable event.

Fifth, the appropriate entities should create or enhance organizations’ behavioral observation programs by incorporating ways to spot visual and verbal extremist identifiers in the workplace. This could be included in behavioral observation training and related materials as well as emphasized as a reporting requirement.

Finally, policymakers need to better address security risks and threats posed by extremists who previously had access to classified or other sensitive information and may be targets of future radicalization and recruitment by extremists. Among other things, this should include updating existing policy frameworks to create a uniform baseline standard for data collection on extremist-related and other motivated insider threats across the entire USG enterprise.
Introduction

Hundreds of thousands of people hold positions of trust in the U.S. federal government (USG), including ones requiring security clearances. It is imperative that those assessing, investigating, and adjudicating government personnel background checks and security clearances have knowledge and interest in ensuring that malicious actors are prevented from joining this trusted workforce. Actors who could pose insider threats (i.e., operational security, counterintelligence, harassment/equal employment opportunity, and reputational risk concerns) to America's government service workforce hold various motivations and come from different backgrounds, including far-right extremism.

In particular, recent actions by individuals in positions of public service with far-right extremist motivations have drawn renewed scrutiny due to their potential as insider threats. Yet the challenge of potential insider threats from far-right extremists is not a recent development; civil society watchdogs and law enforcement agencies have warned the public about this issue for several decades. Discussion of this topic is, however, largely fraught with concerns about political polarization, civil liberties, and privacy. The need for further data collection to better inform our decisionmakers compounds this problem.

This policy report will discuss individuals in USG employment, including those with security clearances, who have ties to far-right extremist movements and activities. The authors focus on far-right actors who potentially pose insider threats due to their underlying ideologies' or movements' sizeable support base and their prior history within the federal security-related workforce.

Background

To the extent far-right extremism is associated with insider threats, what is already known suggests the possibility of a systematic problem...
The clear identification of those who are far-right insider threats and who are not complicates reporting further.

of infiltration into and recruitment from military, law enforcement, and other security-sensitive government service positions. For example, a December 2021 investigation by the Associated Press noted that despite decades of efforts, including recently revised rules and guidance, “racism and extremism remain an ongoing concern in the military.”

Meanwhile, multiple studies and investigative news reports have identified cases of far-right extremist presence within law enforcement entities at local, state, and federal levels.

The clear identification of those who are far-right insider threats and who are not complicates reporting further. For example, while media reports have noted significant numbers of individuals with military backgrounds who allegedly participated in the Jan. 6, 2021, attack against the U.S. Capitol complex, this amounts to approximately 12 percent of the total number of alleged offenders. Moreover, a closer and systematic look at their professional backgrounds indicates few among them were actually in the armed services at the time of their alleged crimes. According to a January 2022 study by the University of Maryland’s START Center, “The vast majority (91%) of Capitol defendants with military backgrounds were no longer serving in the armed forces on Jan. 6, 2021. In fact, on average, the subjects who are facing charges for the Capitol breach have been separated from military service for nearly 15 years.” Properly defining and identifying who are insider threats has direct implications for the policy formation and practice of preventing and countering this security challenge.

Finally, while associated acts of terrorism and other forms of political violence — like Jan. 6, 2021 — have attracted civil society, media, congressional, and federal policymaker attention, insider threats from far-right extremists are not limited solely to direct acts of violence. Information security, operational security, internal workplace morale, and public trust in the core functions of government institutions (i.e., agency or government reputational risk), among other things, are also potentially jeopardized by insider threat activities.

Defining the Scope and Key Terms/Concepts of this Report

Scope

This publication will focus on potential insider threats from far-right extremists who are employed within USG entities. Therefore, issues such as far-right extremists with professional backgrounds in state/local law enforcement or other first-responder entities are outside the scope of this report.

Moreover, we view potentially malicious actors within a simple three-stage framework of employment status in federal government service: 1) pre-service/admittance, 2) current involvement, and 3) post-service. In relation to how “insider” and “insider threat” are defined, this brief will mostly focus on the first two stages of employment status, although post-service individuals (e.g., veterans) will also be discussed to the extent that they impact insider threat policy and practice.

Finally, this report focuses on the two highest security tiers of USG positions: public trust and national security positions (discussed below). These positions — along with non-sensitive, the lowest security tier — are categorized based on the level of risk and sensitivity level of information, information systems, or facilities a person may have access to.

“Insider” and “Insider Threat”

This publication uses the definitions of “insider” and “insider threat” described in the National Insider Threat Policy, or NITP. These definitions were chosen because they were formulated under the aegis of the Insider Threat Task Force, established under Executive
Although several different sub-movements constitute the U.S. far-right, this report largely focuses on white nationalism/supremacy, anti-government extremism, and a specific subset of anti-government extremism called the militia movement. Informing this focus is prior evidence suggesting that these ideologies pose significant insider threats to USG and other government personnel/institutions. Where relevant, other actors representing other far-right sub-ideologies/movements are also discussed.

<table>
<thead>
<tr>
<th>White nationalists/supremacists</th>
<th>Anti-government extremists</th>
<th>Militia extremists</th>
</tr>
</thead>
<tbody>
<tr>
<td>White nationalists/supremacists believe that &quot;white&quot; people are genetically, morally, and/or culturally superior to all other races. They also tend to be overwhelmingly antisemitic. White nationalists/supremacists also express intense hatred toward sexual and gender minorities as well as individuals they deem as &quot;parasites&quot; upon society, such as homeless people.</td>
<td>Anti-government extremists are primarily mobilized by an intense fear and loathing of government actors — especially those representing the USG — rather than ethnic/racial/religious hatred.</td>
<td>Militia extremists share many of the beliefs common to other anti-government extremists, but they emphasize armed paramilitary training and organizational structure in defense against what they see as government threats to citizens’ constitutional rights.</td>
</tr>
</tbody>
</table>

Although representing distinct segments of the U.S. far-right milieu, these sub-movements have been known to overlap with each other in terms of supporters, as well as similar-sounding narratives that justify and inspire their activities, including unlawful violence.

"Non-sensitive," "Public Trust," and "Security Clearance"

There are three security-tiered designations of USG positions: non-sensitive, public trust, and national security (for the sake of clarity, throughout this report "national security" positions will be referred to as "security clearance" positions). These positions are designated based on two factors. First is the risk level associated with position. Risk level identifies what the negative ramifications would be to the agency, the government, and the nation if the person performing this job does something that causes damage or brings discredit upon through an act of negligence, omission, criminal, illegal or unethical behavior or conduct. The three levels of risk for USG positions are low, moderate, and high. The second factor is the sensitivity level associated with the position. Sensitivity means the position requires access to classified national security information, a sensitive facility, and/or an information system with classified information. To be eligible for these positions, applicants are required to obtain a security clearance. There are four levels of sensitivity, in ascending order: 1) Non-Sensitive, 2) Non-Critical Sensitive, 3) Critical Sensitive, and 4) Special Sensitive.
Traditionally, those investigating, adjudicating, and granting security clearances have viewed the threats of extremist entry into and recruitment from within the federal workforce in terms of plots to overthrow the government through force, criminal acts, or violent conduct. It is also important to acknowledge other potentially detrimental aspects of extremists in the federal workforce, such as potential counterintelligence/information security, operational security, and insider threats, when conducting background investigations, adjudications, and suitability determinations.

The three types of security-tiered USG positions can be defined as follows:

<table>
<thead>
<tr>
<th>Non-sensitive positions</th>
<th>Public trust positions</th>
<th>Security clearance positions</th>
</tr>
</thead>
<tbody>
<tr>
<td>They are low-risk and do not require security clearances. Applicants are required to submit a Standard Form (SF) 85 Questionnaire for Non-sensitive Positions.</td>
<td>Public trust positions: They are moderate to high risk and do not require security clearances. Applicants are required to submit a SF-85P Questionnaire for Public Trust Positions.</td>
<td>Security clearance positions: Officially called national security positions, they can be low, moderate, or high risk and require security clearances. Applicants are required to submit a SF-86 Questionnaire for National Security Positions.</td>
</tr>
</tbody>
</table>

Again, non-sensitive positions are outside the scope of this report.

Overview of Personnel Vetting Processes

Dating back to at least the 1950s, personnel vetting processes are used to determine an individual’s trustworthiness and suitability for being in public trust and security clearance positions. There are at least four general steps involved in a vetting process:

1. **Initiation.** A job applicant agrees to submit themselves to a background investigation as part of their application to a government agency employment opportunity. This is typically done by filling out and submitting a questionnaire.

2. **Investigation.** The government agency uses the information submitted by the applicant to scrutinize their background. Investigators will verify information contained in the SF documents, including past and current residences, education, employment history, financial well-being, and criminal records checks. This information is typically supplemented with follow-up in-person interviews of the applicant, their family, friends, and acquaintances.

3. **Adjudication.** Based on the information gleaned from the applicant’s submission and the subsequent investigation, the agency determines if the individual is suitable for government employment as a public servant or private contractor, eligible to access classified information, and eligible for identification to access agency systems and/or facilities. Disqualifying factors can include things like financial insolvency, certain types of criminal offenses, problems with substance abuse, problematic employment history, lying on an official government document (like a Standard Form questionnaire), and/or involvement with adversarial foreign contacts that could compromise an applicant’s ability to safeguard sensitive U.S. information and other assets.

4. **Post-adjudication.** If provided an unfavorable adjudication, the applicant typically has the right to appeal their case before the appropriate administrative court. If given favorable adjudication, the individual will be subject to periodic reinvestigation to maintain suitability and clearance for their position. Depending on the risk level and sensitivity associated with the position, employees are required to be reinvestigated at least once every five, 10, or 15 years. In some cases, an individual may be eligible for continuous vetting, which involves automated and semi-automated background checking.

Traditionally, those investigating, adjudicating, and granting security clearances have viewed the threats of extremist entry into and recruitment from within the federal workforce in terms of plots to overthrow the government through force, criminal acts, or violent conduct. It is also important to acknowledge other potentially detrimental aspects of extremists in the federal workforce, such as potential counterintelligence/information security, operational security, and insider threats, when conducting background investigations, adjudications, and suitability determinations.
Manifestations of Insider Threats and Their Link to Far-Right Extremists

Insider threats can manifest in a multitude of ways, including:

- Espionage
- Terrorism
- Unauthorized disclosure of information
- Corruption
- Sabotage
- Workplace violence
- Intentional or unintentional loss/degradation of departmental resources or capabilities

What this list shows is that insider threats driven by various motives potentially pose both kinetic (physical use of force) and non-kinetic (latent or unconventional methods) insider threats. Extremist insider threats could jeopardize the physical protection of a government building, physically threaten the lives of personnel, compromise law enforcement investigations, tip off potential suspects that belong to a shared extremist group or movement, obstruct operations such as a search or arrest warrant, or leak classified or sensitive information, among other scenarios.

In some cases, the presence of alleged far-right extremist insiders posed a potential threat but did not materialize directly into violence. For example, during preparation for the presidential inauguration after the contested 2020 national elections, two National Guardsmen assigned to protect the Capitol after the Jan. 6, 2021, insurrection were removed from their protection duties for possible links to far-right extremist movements. Even if these two individuals posed no actual problem, the mere possibility of a potential insider threat clearly imposed logistical and personnel costs as well as investigative resources for it to be properly mitigated.

In other cases, evidence suggests that insider threats have materialized from far-right extremists and their supporters in government positions. In February 2022, the Washington D.C. Metropolitan Police Department (MPD) suspended 22-year law enforcement veteran Shane Lamond for alleged inappropriate ties to the far-right extremist group Proud Boys. Lamond, who worked in the MPD’s Intelligence Bureau at the time of his suspension, is suspected of having ties to former Proud Boys leader Henry “Enrique” Tarrio and sending him information on the locations of counterdemonstrators. While Tarrio claims the information was meant to avoid violent encounters, The Washington Post notes, “police accused the Proud Boys of roaming the city looking for and instigating fights, targeting people they believed identified as antifa, or antifascists.”

The matter, as of this writing, remains under investigation by the MPD, FBI, U.S. Department of Justice, and the U.S. Attorney’s Office for the District of Columbia.

As illustrated in this example, far-right extremists in the federal workforce pose a challenge that goes beyond violence or other unlawful acts typically associated with insider threats. Driven by various motives, insider threats could also disrupt the workplace in other ways, such as leaking sensitive information, harassing staff, or violating equal employment opportunity or other agency policies. Some domestic extremist movements, like white supremacy, are centered on overt racist, sexist, and other bigoted beliefs that raise questions about extremists’ ability to engage with service recipients and workplace colleagues of different backgrounds in a professional, lawful, and unbiased manner. Even if individuals who hold such beliefs express them lawfully outside the workplace, the knowledge of their presence within the federal workforce could undermine staff morale or public confidence in that department or agency. While this brief focuses on potential insider threats posed by far-right extremists, its insights potentially hold lessons for preventing and mitigating other forms of extremist-associated insider threats, too.

Activities of Far-Right Extremists with Public Trust/Security Clearance Positions

A broad range of domestic extremists, most notably far-right extremists, have held positions with law enforcement, military, or government agencies and institutions at all levels. Some of these extremists may have security clearances or access to sensitive law enforcement and other government information. The following extremist movements have demonstrated a recurring
ability to recruit members and supporters from personnel working in public trust and security clearance positions. Based on a review of court documents, non-government publications, and media reporting, these movements are thought to be most likely to have members serving in public trust and security clearance positions that put them in close physical proximity or direct access to sensitive information, facilities, or information systems.

**Anti-government Extremists**

Anti-government groups such as the Oath Keepers and Constitutional Sheriffs and Peace Officers Association, or CSPOA, are open about their efforts to recruit members of law enforcement and the military.

In November 2020, Atlantic Magazine exposed a verified Oath Keepers membership roster indicating the group had recruited 25,000 police, soldiers, veterans, and emergency response officials across all levels of government. In September 2022, the Anti-Defamation League published an analysis of leaked Oath Keeper recruitment and membership data on more than 38,000 individuals. They identified...
hundreds of people they believe are currently serving in military services as well as law enforcement and other first responder institutions. While taking into consideration that many likely signed up and never participated actively, data presented in the report strongly suggests several of the individuals listed in the Oath Keepers database were actively involved in the group while employed in public trust-type positions within law enforcement, the military, first responders, or other national security/public safety-relevant entities.

Meanwhile, investigative reporting by anti-hate watchdog groups Anti-Defamation League and Political Research Associates has identified significant inroads made by CSPOA and the wider “Constitutional Sheriffs” movement into mainstream sheriff’s departments and associations. Given their prevalence in several parts of the United States, entities led by so-called “Constitutional Sheriffs” may have access to federally supported fusion center networks or have personnel assigned to FBI-led Joint Terrorism Task Forces. These fusion centers and task forces often require local and/or state law enforcement personnel to have security clearances prior to their assignment.

Militia Extremists

Examples include the FEAR (Forever Enduring, Always Ready) militia, a group that formed in 2011 at U.S. Army base Ft. Stewart, in Georgia. Its members were motivated by a mix of personal grievances against the military and extremist ideology. Four of its members, including its leader, were convicted of murder-related charges, while nine others were sentenced on various drug, weapons, and other charges. Their leader, Isaac Aguigui, was assigned to a U.S. Army intelligence unit and had a security clearance.

In 2013, a commander of a Minnesota militia, Keith Michael Novak, who reportedly was trained in intelligence gathering by the U.S. Army and serving in the National Guard, was arrested by the FBI for stealing classified information. Novak allegedly had intended to use the information as part of a wider scheme to provide fake identities to other militia members and to steal sensitive military gear and equipment. He was sentenced to two years in prison and later convicted and sentenced to 12 years for possession of child pornography found during the initial investigation into his theft of classified material.

Other actors, like the once-active “Boogaloo” movement, inspired violent extremists like Steven Carrillo. In two separate incidents over an eight-day span in late May and early June 2020, Carrillo—an active-duty Air Force staff sergeant who was the leader of a highly trained team of Air Mobility Command Phoenix Raven security forces—fatally shot two federal and local law enforcement officers and wounded five others.

White Supremacists/Nationalists

In the past, white supremacists/nationalists have received periodic scrutiny from law enforcement organizations, government agencies, and military services during vetting of new applicants due to their longstanding attempts to infiltrate such organizations. In 2018, a Metro Transit Police Department officer named Nicholas Young, who simultaneously held neo-Nazi and jihadist views, was convicted of providing material support to the Islamic State militant group.

Rinaldo Nazzaro, former leader of the neo-Nazi accelerationist group “The Base,” reportedly worked at the U.S. DHS Office of Intelligence and Analysis as an intelligence analyst from 2004 to 2006 and as a private contractor with U.S. special forces in the Middle East in 2014. In 2018, Nazzaro reportedly left the United States for St. Petersburg, Russia, to organize and lead the neo-Nazi group. According to a Feb. 17, 2021, Telegram post attributed to Nazzaro, he developed white supremacist/nationalist beliefs toward the end of his career in national security, which he claims led him to eventually quit the field. This suggests there was some chronological overlap between his access to sensitive information, information systems, and/or facilities while in government service and his eventual embrace of white supremacism/nationalism.

On Feb. 15, 2019, a U.S. Coast Guard lieutenant named Christopher Hasson was arrested following a multi-year investigation of his activities, including use of USG information systems. He was later convicted in Maryland on four federal charges related to narcotics and firearms violations.
and sentenced to 160 months in federal prison. Although Hasson was never formally charged with terrorism-related offenses, prosecutors labeled him a “domestic terrorist.” Investigators found evidence that Hasson self-identified as a white nationalist, stockpiled weapons, advocated for “focused violence” to establish an all-white homeland and developed lists of potential targets to attack including media figures, as well as former and current elected officials. According to media reporting of court documents and a backgrounder on the case by the Defense Counterintelligence and Security Agency, he worked in acquisitions for national security cutter boats and obtained a Secret Clearance but was denied a Top Secret/Sensitive Compartmentalized Information status.

In 2020, an Army soldier from Louisville, Kentucky, was arrested by the FBI for reportedly giving classified information to a European neo-Nazi group called “the Order of Nine Angels,” which was then intended to be sent on to jihadists for the purposes of facilitating a terrorist attack against fellow soldiers. He was convicted on charges related to attempted homicide of military personnel, material support for terrorism, and espionage.

Investigative research published in November 2021 identified Brian P. Haughton, a former member of two high-profile bands in the neo-Nazi music scene, as a 22-year veteran of the Philadelphia Police Department and employee at the U.S. Department of Justice-supported Regional Information Sharing System. Law enforcement and criminal justice professionals in all 50 U.S. states and several foreign countries use information shared through this system, including information concerning counterterrorism. It is unclear if Haughton remained a neo-Nazi group member when he entered law enforcement or if he ever improperly disclosed law enforcement sensitive information. Yet his case and others bring further attention to the possibility of far-right extremist presence within policing entities compromising the integrity of intelligence streams and information systems.

Finally on Aug. 26, 2022, following an investigation by the FBI, Killian Ryan was arrested for knowingly making a false statement on a security clearance application form and was discharged from the Army that same day. Ryan was a paratrooper with a secret security clearance level. The investigation revealed ties to unnamed white supremacist organizations and neo-Nazi ideology, as well as one social media post in which the suspect stated his intent to serve in the military was to become “more proficient in killing [African-Americans].”

Other Far-Right Actors and Beliefs

In addition to white supremacy/nationalism and anti-government extremism, there are other beliefs common to various far-right ideologies, such as xenophobia, sexism, and anti-Muslim hate, which pose potential insider threats to USG personnel and institutions. One of the most prominent examples was the “I’m 10-15” private Facebook group for current and retired Border Patrol agents, which had 9,500 members. Investigative reporting revealed numerous comments and memes posted in the group expressing homophobia, xenophobia, and sexism, suggesting a wider current within the organization rather than a handful of isolated individuals. Occasionally this has spilled over into violence against undocumented immigrants, such as when former Border Patrol agent Matthew Bowen hit a fleeing Guatemalan migrant with his truck while on duty. Two weeks prior to the incident Bowen had referred to immigrants as “subhuman” and “mindless murdering savages.”
He later resigned from his job and was sentenced to three years of probation by a federal court.64

Media reporting on the secret group noted that these sentiments potentially affected not only how some Border Patrol agents see and treat undocumented immigrants but also how they treat other agents within their ranks. For example, group members had published anti-LGBTQ posts attacking an openly gay agent who supported Hillary Clinton during the 2016 elections. Sexist posts at minimum reinforce what critics have argued is a widespread organizational culture of misogyny and point to empirical evidence that shows only 5% of its agents were female — the lowest ratio among all U.S. federal law enforcement agencies surveyed by Politico in 2017.65

Beyond the Border Patrol’s issues, significant controversy and concern has erupted over anti-terrorism trainings containing explicit anti-Muslim content provided by far-right extremist activists and pseudo-experts to other federal law enforcement agencies, private security companies guarding federal facilities, and military services.66 While research identifying the direct effects of these trainings is sparse, what is known suggests they potentially inform threat assessments made by people who are not only public servants in positions of trust but also the targets of far-right propaganda and recruitment.67 Misinformed by extreme beliefs and disinformation under the guise of anti-terrorism training, these public servants could be influenced to see a person’s race or religion as the key factor in deciding whether the person poses a threat, then influence and/or reinforce policymakers’ decisions. These assessments also affect the operational behaviors of front-line personnel (e.g., surveilling certain types of individuals based on their background rather than individualized suspicion of criminal wrongdoing).68 In other cases, such trainings at minimum appear to reinforce existing organizational work cultures that are alleged to be hostile to Muslims and other minorities.69

In at least one case, such trainings directly led to a federal law enforcement officer of Muslim background filing a complaint with the Equal Employment Opportunity Commission, which later ruled in the officer’s favor.70

Policy Recommendations

Policymakers in government and decisionmakers in civil society should consider these steps to mitigate the risk of violence, unauthorized disclosure of information, and compromise of sensitive public safety/national security assets from insider threats motivated by far-right extremism:

First, the U.S. Intelligence Community, led by the FBI and assisted by the DOJ, the DHS, and National Counterterrorism Center, must revisit and, if needed, revise strategies to deal with operational security concerns related to extremists employed in law enforcement, the U.S. military, and government (specifically at the federal level). While a federal policy framework to address insider threats exists, recent events, as documented in this publication, suggest it would be wise to revisit the matter to see if existing policy and practice is suited for the current challenge of insider threats by far-right extremists.71 This should include the possibility of declaring specific extremist movements and groups as potential national security threats to give security professionals clarity about which actors pose potential insider threats. It should also include policy guidance on a uniform baseline data collection standard on extremist-related and other motivated insider threats across the entire USG enterprise.

Second, security professionals involved in government security vetting processes need basic training related to far-right extremism. This will assist security professionals involved with investigating, adjudicating, and maintaining individuals’ security clearances with gaining a better understanding about why and how extremists pose public safety and national security threats.

Third, the Office of Personnel Management, the Defense Counterintelligence and Security Agency, and other government agencies/organizations responsible for investigating, adjudicating, maintaining, and updating access to public trust and security clearance positions should:

- Consider adding and/or revising questions on clearance application forms such as the U.S. government’s Standard Forms (SF) 85P and 86
Questionnaires — including their Association Record components — to capture applicant responses related to extremist participation beyond terrorist organizations or subversive groups wanting to overthrow the government by force, which are the only criteria in the current SF85P and SF86 Questionnaires.

- Clarify and institute policies to enable background investigators and other security officials to access social media posts and other publicly available information that could identify extremist affiliations and activities of concern, per FBI/DHS and other relevant agency training.

- Ensure that continuous evaluation programs and other vetting initiatives identify new information regarding trusted employees’ extremist affiliations and activities of concern, per FBI/DHS and other relevant agency training.

Fourth, the Office of Personnel Management, the Defense Counterintelligence and Security Agency, and other government agencies and organizations involved in vetting processes should consider making an employee’s participation in, affiliation with, or support for extremist groups/movements/causes that advocate violence against USG officials or property a reportable event. Currently, individuals holding a security clearance must report activities...
such as a change in marital status, foreign travel, drug use, or arrest to their staff security officer or face possible administrative action or fine. There is, however, no reporting requirement for extremist affiliation or participation. Behavioral observation is an important aspect of agency counterintelligence and other insider threat mitigation programs. Reporting visual and verbal identifiers related to extremism should be incorporated into these programs.

Fifth, create or enhance organizations’ behavior observation programs by including how to recognize visual and verbal extremist identifiers in the workplace. This could be folded into behavioral observation training and related materials and emphasized as a reporting requirement. Further, misuse of government computers to view, listen to or watch extremist propaganda the workplace could be another reportable extremist behavior. Various critical infrastructure sectors and some government agencies have developed behavioral observation programs to observe and report certain designated behaviors that may have an adverse effect on safety or security at their facilities. Examples of reportable workplace behaviors may include drug or alcohol use, psychological conditions, fatigue, criminal activities, and terrorism. Training staff to notice various signs of extremism, such as terminology and symbology unique to extremist groups, would enhance behavior observation programs. These programs could be implemented more broadly across government agencies.

Finally, policymakers need to better address security risks and threats posed by people who previously had inside access to sensitive or other classified information and may be targets of future radicalization and recruitment by extremists. USG insider threat policies are designed to address malicious actors seeking entrance to government service or removing their threats if they are already in public trust/security clearance positions, with little attention given to those who have left government service. In theory, this may make sense because when a person does not have privileged access, they are, by definition, not an “insider.” In practice, these theoretical boundaries are not so clear-cut. People who served in USG public trust and security clearance positions do not automatically forget their professional knowledge, skills, and abilities upon discontinuing their public service. The example of Rinaldo Nazzaro shows that while he probably constituted a potential insider threat toward the end of his U.S. national security career, once he left the field, he immediately used his professional know-how to advance violent extremist goals. Other examples extend to the dozens of veterans — such as several of the alleged Jan. 6 insurrectionists, including the individual who attacked the FBI field office in Cincinnati on Aug. 11, 2022 — who were discharged from military service several years before engaging in political violence. Policymakers are therefore urged to devise comprehensive policy frameworks and coordinated interagency programmatic efforts that protect former USG insiders from plausible recruitment and radicalization efforts by extremists.

Steps Taken, Steps Ahead

The Intelligence community has recently developed a comprehensive threat assessment for domestic terrorism, and the Biden administration has developed a National Strategy for Countering Domestic Terrorism. These efforts are merely the first steps in combating domestic terrorism. The Department of Justice, FBI, and DHS should provide guidance to security professionals in government service on how to determine which domestic extremist groups or movements pose a threat to national security so they can better investigate, adjudicate and maintain integrity with issuing government clearances.

Administrative actions and discipline are necessary against identified extremists with government public trust and security clearance positions (e.g., their access restricted or revoked, downgraded, or suspended; reassignment to a different position; or termination of employment). Government computer systems (particularly business networks) should be routinely monitored for violations of policies such as indications of fraud, waste, and abuse of government time and property as it relates to extremist content. Also, better monitoring of agency
EEO and harassment programs for allegations of racism and sexism are needed to see if there are any extremist affiliations or connections. Finally, unacceptable behavior and activities identified as related to national security vulnerabilities, risk, and threats must be balanced with employees’ right to privacy and civil liberties.

Extremists are currently serving in sensitive government positions, and many others have had past access to those positions. This clearly shows there is more work to be done with screening potential applicants for these positions as well as assessing the potential insider threat posed by those already employed who have ties to extremist groups or support their causes. Not acting on these recommendations allows this threat to persist and likely grow in our nation’s highly sensitive and trusted places where they should not exist.

**Daryl Johnson** is one of the foremost experts on domestic extremist groups in the United States and a nonresident fellow with the New Lines Institute for Strategy and Policy. Beginning his career as a civilian in the U.S. Army, Johnson has held several government positions, most recently as senior analyst at the Department of Homeland Security. He is also regularly cited, featured, or quoted in media covering domestic extremist groups in the United States, including the New York Times, Washington Post, Wall Street Journal, Newsweek, National Public Radio, MSNBC, CNN, and NBC Nightly News, among many others. He is the author of “Hateland: A Long, Hard Look at America’s Extremist Heart” (Prometheus Books, 2019) and “Right-Wing Resurgence: How a Domestic Terrorism Threat Is Being Ignored” (Rowman & Littlefield, 2012).

**Alejandro J. Beutel** is a nonresident fellow with the New Lines Institute for Strategy and Policy who studies non-violent and violent far-right extremist and Islamist movements. Beutel is a former Senior Research Analyst at the Southern Poverty Law Center and a former Researcher for Countering Violent Extremism at the University of Maryland’s National Consortium for the Study of & Responses to Terrorism. He is also a doctoral candidate in Criminology at the University of Massachusetts Lowell.
Endnotes


2 For example, in July 2022, along a mostly party line vote, a 14-12 majority in the Senate Armed Services Committee (SASC) opposed the Pentagon's ongoing efforts to combat “extremism” in its ranks. See: Williams, J. (2022, July 20). Senate defense bill signals opposition to Pentagon's extremism efforts. The Hill. https://thehill.com/policy/defense/3567244-senate-defense-bill-signals-opposition-to-pentagon-extremism-efforts.


Although purportedly based on biology, race is in fact a social construct. Here it is worthwhile to refer to insights from Biological Anthropology.

Under the authorities and efforts of the Task Force, federal entities may have insider threat standards and operating procedures tailored to their particular needs, however they also share certain basic operating norms and principles across various departments/agencies.

Because of that, over the last five centuries, race has become thus does not have its roots in biological reality, but in policies of discrimination.

Claimed biological reality, but in policies of discrimination. It be understood as a classification system that emerged from, and in support of, European colonialism, oppression, and discrimination. It...

53 Reilly, R. J. (2020, January 31). *Christopher Hasson sentenced to more than 15 years in domestic terrorism plot.* HuffPost. https://www.huffpost.com/entry/christopher-hasson-sentenced-domestic-terrorism-n_5e343ec7b69a1b4a46a9/


68 Among those stories, which included Barodi’s, were accounts of white FBI officials who exhibited blatant anti-Muslim bias. In 2016, Comey held a meeting with representatives of minority groups at the FBI, including African Americans, Muslims, women, Asian Americans, and LGBT employees. He heard what Barodi called the ‘struggle stories’ of nine different Muslim employees who have faced what they consider discrimination. Among those stories, which included Barodi’s, were accounts of white FBI officials who exhibited blatant Islamophobia, including those who blamed terrorism on Islam and suspected their Muslim colleagues of adherence to sharia law over the US constitution.” (emphasis added) Blaming the Islamic faith and/or Muslims writ large, rather than a particular interpretation of it by a minority of violent individuals for acts of terrorism, as well as allegations of Muslims’ disloyalty to America based on their adherence to sharia are common conspiracy theories frequently found in anti-Muslim training presentations to law enforcement, military, and other security service professionals. See: Schachtman, N., & Ackerman, S. (2012, May 10). *U.S. military taught officers: Use ‘Hiroshima’ tactics for ‘Total war’ on Islam.* Wired. https://www.wired.com/2012/05/total-war-islam/


70 Among those stories, which included Barodi’s, were accounts of white FBI officials who exhibited blatant anti-Muslim bias. In 2016, Comey held a meeting with representatives of minority groups at the FBI, including African Americans, Muslims, women, Asian Americans, and LGBT employees. He heard what Barodi called the ‘struggle stories’ of nine different Muslim employees who have faced what they consider discrimination. Among those stories, which included Barodi’s, were accounts of white FBI officials who exhibited blatant Islamophobia, including those who blamed terrorism on Islam and suspected their Muslim colleagues of adherence to sharia law over the US constitution.” (emphasis added) Blaming the Islamic faith and/or Muslims writ large, rather than a particular interpretation of it by a minority of violent individuals for acts of terrorism, as well as allegations of Muslims’ disloyalty to America based on their adherence to sharia are common conspiracy theories frequently found in anti-Muslim training presentations to law enforcement, military, and other security service professionals. See: Schachtman, N., & Ackerman, S. (2012, May 10). *U.S. military taught officers: Use ‘Hiroshima’ tactics for ‘Total war’ on Islam.* Wired. https://www.wired.com/2012/05/total-war-islam/


76 Although this occurs in places such as the Department of Defense, Intelligence Community, and several USG law enforcement agencies, the authors believe this point nevertheless bears emphasis. One of the authors of this publication (Johnson) who is also a USG employee with over 30 years of intelligence and homeland security experience, wishes to point out that “Non-Title 50 organizations” (i.e., federal departments/agencies, writ-large not listed as elements of the U.S. Intelligence Community, but who have intelligence units within them that have access to the IC) do not have the resources to routinely monitor their classified and business networks as much as one might presume. Several Title 50 entities also do not typically perform routine monitoring unless a problematic employee has already been identified. For an overview of Title 50 and Non-Title 50 entities, see: Wagner, C., Alexander, B., Bamford, G., Choi, A., Coffey, A., Farkus, C., Hunt, D., Jameson, G., Johnson, L. M., Kim-Mitchell, E., Loren, D., Nacos, J., Renga, J., Scalisi, D., Smith, J., Spadoro, T., Steinier, J., Van Duyn, D., & Woolsey, M. (2016). *Protecting the homeland: Intelligence integration 15 years after 9/11*. Intelligence and National Security Alliance. https://www.insaonline.org/wp-content/uploads/2017/04/INSA_WP_ProtectHomeland.pdf.
Contact

✉️ For media inquiries, email media@newlinesinstitute.org
✉️ To submit a piece to the New Lines Institute, email submissions@newlinesinstitute.org
✉️ For other inquiries, send an email to info@newlinesinstitute.org

📍 1776 Massachusetts Ave N.W. Suite 120
   Washington, D.C. 20036
📞 (202) 800-7302

Connect With Us

@newlinesinst | @New Lines Institute for Strategy and Policy | Subscribe | Sign up