Volume 230 Issue 4 2023

MILITARY LAW REVIEW

Articles

Lecture

Academic Journal No. 27-100-230-4

Military Law Review

Volume 230 **Issue 4** **2023**

CONTENTS

Headquarters, Department of the Army, Washington, D.C.

Academic Journal No. 27-100-230-4, 2023

Military Law Review

Volume 230
Issue 4

Since its inception in 1958 at The Judge Advocate General's School, U.S. Army, in Charlottesville, Virginia, the *Military Law Review* has encouraged a full and frank discussion of legislative, administrative, and judicial principles through a scholarly examination of the law and emerging legal precepts. In support of that mission, the *Military Law Review* publishes scholarly articles that are relevant to, and materially advance, the practice of law within the military.

The *Military Law Review* does not promulgate official policy. An article's content is the sole responsibility of that article's author, and the opinions and conclusions that are reflected in an article are those of the

author and do not necessarily reflect the views of the U.S. Government, the Department of Defense, the Department of the Army, The Judge Advocate General's Corps, The Judge Advocate General's Legal Center and School, or any other governmental or non-governmental agency.

WEBSITE: The *Military Law Review* is available online at https://tjaglcs.army.mil/mlr.

CITATION: Cite this issue of the *Military Law Review* as 230 MIL. L. REV. [page number] (2023).

MANUSCRIPT SUBMISSIONS: The *Military Law Review* accepts manuscript submissions from military and civilian authors. Any work submitted for publication will be evaluated by the *Military Law Review*'s Board of Editors. In determining whether to publish a work, the Board considers the work in light of the *Military Law Review*'s mission and evaluates the work's argument, research, and style.

No minimum or maximum length requirements exist. Footnotes should be numbered consecutively from the beginning to the end of the manuscript rather than by section. Citations must conform to *The Bluebook: A Uniform System of Citation* (21st ed. 2020) and the *Military Citation Guide* (25th ed. 2022). Submissions should include biographical data for each author, to include branch of service, duty title, present and prior positions or duty assignments, all degrees (with names of granting schools and years received), and previous publications. If submitting a lecture or paper prepared in partial fulfillment of degree requirements, the author should include the date and place of delivery of the lecture or the date and source of the degree.

Submissions must be in Microsoft Word format and should be sent via email to the Editor, *Military Law Review*, at usarmy.charlottesville.hqda-tjaglcs.mbx.military-law-review@army.mil. If email is not available, please forward the double-spaced submission to the Editor, *Military Law Review*, Administrative and Civil Law Department, The Judge Advocate General's Legal Center and School, U.S. Army, 600 Massie Road, Charlottesville, Virginia 22903-1781.

MILITARY LAW REVIEW

Volume 230 **Issue 4**

RULES OF ENGAGING IN FOREIGN DISASTER RELIEF: A PROPOSAL

MAJOR LESLIE M. SCHMIDT*

I. Introduction—A Hypothetical[1]

Typhoon Acadia struck the Philippines with astounding force, dropping twelve inches of rain in the first twelve hours of the storm in some areas, with winds topping two hundred miles per hour. Eastern Mindanao took a direct hit, sustaining extensive damage to infrastructure, including 98 percent power outages, flooded roads, and no access to clean

* Judge Advocate, U.S. Army. Presently assigned as Staff Judge Advocate, Special Operations Command-Korea, Camp Humphreys. LL.M., 2022, The Judge Advocate General's Legal Center and School, United States Army; J.D., 2011, University of Virginia; B.A., 2006, The College of William & Mary. Previous assignments include Group Judge Advocate, 4th Psychological Operations Group (Airborne), Fort Liberty (formerly known as Fort Bragg), North Carolina, 2020–2021; Command Judge Advocate, 16th Military Police Brigade, Fort Liberty, North Carolina, 2018–2020; Operational Law Attorney, U.S. Army Africa/Southern European Task Force, Vicenza, Italy, 2017–2018; Operational and Administrative Law Attorney, 173d Infantry Brigade Combat Team (Airborne), Vicenza, Italy; Trial Counsel, 17th Field Artillery Brigade, Joint Base Lewis-McChord, Washington, 2014–2015; Legal Assistance Attorney, 7th Infantry Division, Joint Base Lewis-McChord, Washington, 2013; Administrative Law Attorney, 7th Infantry Division, Joint Base Lewis-McChord, Washington, 2012–2013. Member of the Virginia State Bar. This paper was submitted in partial completion of the Master of Laws requirements of the 70th Judge Advocate Officer Graduate Course. The views expressed herein do not necessarily represent the views of the Department of the Army, Department of Defense, or any other department of the U.S. Government.

[1] This scenario is fictional but loosely based on real-world natural disasters and risk assessments conducted for climate-change-related disaster. *See* DAVID ECKSTEIN ET AL., GLOBAL CLIMATE RISK INDEX 2021, at 13–14 (2021) [hereinafter GCRI 2021]; CLIMATE CHANGE COMM'N, CLIMATE CHANGE AND THE PHILIPPINES EXECUTIVE BRIEF 2018-01 (2018).

water for most of the population. The Philippine government estimates that the storm displaced sixteen million people due to flooding and destruction of homes. The death toll has reached seven thousand and is climbing as thousands more are reported missing. The world community rallies to support the Philippines, and the U.S. Bureau for Humanitarian Assistance requests Department of Defense (DoD) assistance in its relief efforts.[2] The U.S. Army's 7th Infantry Brigade Combat Team (7th IBCT), 25th Infantry Division, fresh from the Jungle Operations Training Course, [3] is at Wheeler Army Airfield waiting to board planes and deploy in support of the foreign disaster relief (FDR) mission.[4]

Despite the U.S. Government's (USG) eagerness to assist, there is still some concern due to the real-world history between the United States and the Philippines. The United States colonized the Philippines from 1898 to 1946.[5] During the colonization period, hundreds of thousands of civilians died due to war, famine, and disease.[6] After Philippine independence, the United States' permanent military presence in the country continued until 1992. [7] This history continues to color modern relations with the Philippines.

Today, the United States views the Philippines as an important partner in Southeast Asia. The United States-Philippines Mutual Defense Treaty has been in effect since 1951, and U.S. strategy frames this alliance as key to a "free and open Indo-Pacific."[8] It is home to more than 300,000

---

[2] The Bureau for Humanitarian Assistance replaced the Office of U.S. Foreign Disaster Assistance (OFDA) in 2020. Because this change is recent, U.S. Department of Defense (DoD) policy and regulations have not caught up; therefore, OFDA will be referenced in this paper when citing older references or detailing OFDA historic actions. *Bureau for Humanitarian Assistance*, U.S. AGENCY FOR INT'L DEV., https://www.usaid.gov/who-we-are/organization/bureaus/bureau-humanitarian-assistance (last visited Apr. 10, 2023).

[3] "The 25th ID Jungle Operations Training Course (JOTC) focuses on jungle mobility training, waterborne operations, combat tracking, jungle tactics, survival training, and situation awareness exercises at the Squad level." LIGHTNING ACAD., 24TH INFANTRY DIV., JUNGLE OPERATIONS TRAINING COURSE: COURSE DESCRIPTION AND JOINING INSTRUCTIONS.

[4] The 7th Infantry Brigade Combat Team IBCT is a notional unit stationed at Schofield Barracks, Hawaii.

[5] STANLEY KARNOW, IN OUR IMAGE: AMERICA'S EMPIRE IN THE PHILIPPINES 436-37 (1989).

[6] *Id.* at 194, 287–322 (describing how death associated with the Philippine-American War and the Japanese occupation of the Philippines during World War II (WII) continues to influence the opinions of the Filipino population regarding U.S. presence in the country).

[7] *US-Philippine Joint Statement*, 2 U.S. DEP'T OF STATE DISPATCH 544, 544 (1991).

[8] Mutual Defense Treaty, Phil.-U.S., Aug. 30, 1951, 3 U.S.T 3947; *Fact Sheet: Indo-Pacific Strategy of the United States*, THE WHITE HOUSE, (Feb. 11, 2022), https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/02/11/fact-sheet-indo-pacific-strategy-of-the-united-states (stating the U.S.-Philippines Mutual Defense Treaty is one of five such treaties the United States has in the Indo-Pacific, a region whose security is necessary to support U.S. vital interests).

American citizens, including many U.S. military veterans.[9] The United States helped the Philippine government restore its infrastructure following several natural disasters over the last decade, providing millions of dollars in disaster relief and recovery funds.[10] In addition to natural disasters, the Philippine government struggles with multiple threats to national security, including separatist groups on the island of Mindanao, terrorist organizations including a branch of the Islamic State, and friction with China over sovereignty disputes in the South China Sea.[11] In recent years though, the Philippine government has sought to develop a more positive relationship with China, which runs the risk of degrading U.S.-Philippine military cooperation.[12]

As the 7th IBCT waits for C-130 aircraft to take them to the Philippines, the brigade judge advocate (BJA) jumps on top of a pallet of ruck sacks and briefs the rules of engagement (ROE). The Soldiers dutifully take their ROE cards, noting that they look nearly identical to the cards they received during jungle warfare training the month prior. After the unit gets settled in the Philippines on the island of Mindanao, Alpha Company gets its first mission: providing force protection to engineers rebuilding a road allowing civilians to access supply points. The brigade intelligence officer briefs the commanders that separatist groups in the area have established a pattern of attacking and robbing supply points.

As the engineers work, the Alpha Company commander hears voices and people moving in the jungle to either side of the road. Earlier, he heard gunfire ahead of the group. Convinced that an ambush is imminent, he sends a team forward to scout the area. The team is moving through dense jungle when a man carrying a machete steps out in front of them, yelling in Visayan and gesticulating with a machete. The team engages him with

---

[9] *U.S. Relations with the Philippines: Bilateral Relations Fact Sheet*, U.S. DEP'T OF STATE (Feb.. 23, 2023), https://www.state.gov/u-s-relations-with-the-philippines.

[10] *Id.*

[11] *The World Factbook-Philippines*, CENT. INTEL. AGENCY, (Apr. 4, 2023), https://www.cia.gov/the-world-factbook/countries/philippines.

[12] Jim Garamone, *Philippine President Restores Visiting Forces Agreement with U.S.*, DOD NEWS (July 30, 2021), https://www.defense.gov/News/News-Stories/Article/Article/2713638/philippine-president-restores-visiting-forces-agreement-with-us (discussing threats by President Duterte to cancel the Philippines-United States Visiting Forces Agreement, which is vital to the strong bilateral military relationship between the two countries); Press Release, Dep't of Def., Readout of Secretary of Defense Lloyd J. Austin III's Meeting with Philippine Secretary of National Defense Delfin Lorenzana (Sept. 10, 2021), https://www.defense.gov/News/Releases/Release/Article/2771441/readout-of-secretary-of-defense-lloyd-j-austin-iiis-meeting-with-philippine-sec/ (announcing that the Secretary of Defense (SecDef) has reaffirmed the U.S.-Philippine alliance and their joint mission to secure peace and prosperity in the Indo-Pacific).

lethal force then hears branches snap to their right. Fearing they have stumbled on an ambush, they turn but hold their fire when they see a family carrying water jugs.

The resulting Army Regulation 15-6 investigation finds that no one in 7th IBCT acted wrongfully.[13] The joint force command team developed the ROE per joint doctrine, and the BJA correctly briefed them.[14] In compliance with the ROE, the company commander sent scouts to investigate a potential threat to the unit. And those scouts, based on the information they had at the time, perceived hostile intent and used proportionate and necessary means to neutralize that threat.

Unfortunately, the Philippine government and international community do not feel the Army investigation absolves the unit. Local media publishes that the man with the machete was trying to warn the Soldiers of landmines in the jungle and when they came across him trying to safely guide a family to the road. The photographs of the dead man and crying children, taken by a photojournalist embedded with the engineer group, go viral. The international media is swift and merciless. Stories showing protests and anti-American graffiti are all over the news. The area is now so dangerous that DoD forces and most USG civilians are withdrawing. Multiple Filipino news outlets bemoan the reinstatement of U.S. military power in the area, claiming that the humanitarian mission was a ruse. Official statements from the Chinese government paint a picture of imperialist Americans, massacring the native population, while portraying Chinese intervention as benevolent aid, building capacity in the Philippines. Social media explodes with calls to not trust the United States, cancel defense treaties, and expel USG personnel.

II. A Proposal

The operational environment is always changing. United States competitors are dissecting military action and using it to create their own narrative, highlighting the vulnerabilities of using the wrong paradigm for the use of force on humanitarian missions. Rules of engagement are

---

[13] U.S. DEP'T OF ARMY, REG. 15-6, PROCEDURES FOR ADMINISTRATIVE INVESTIGATIONS AND BOARDS OF OFFICERS (1 Apr. 2016). In the U.S. Army, this regulation establishes procedures for conducting investigations when other regulations or directives do not prescribe different procedures. *Id.* para. 1-1.

[14] Joint doctrine recommends the use of the standing rules of engagement (SROE) to develop guidance for the use of force in foreign disaster relief (FDR) missions. JOINT CHIEFS OF STAFF, JOINT PUB. 3-29, FOREIGN HUMANITARIAN ASSISTANCE, at IV-18 (14 May 2019) [hereinafter JP 3-29].

inappropriate and counterproductive for FDR missions because they emphasize defeating enemies and winning U.S. wars. Alternatively, rules for the use of force (RUF) balance de-escalation and respect for human rights with a commander's inherent right of unit self-defense, aligning it closely with the purpose and mission of FDR.[15] This paper argues that strategic guidance must empower commanders to apply RUF to FDR missions rather than ROE, and, therefore, the Joint Chiefs of Staff must update doctrine applicable to foreign humanitarian assistance and the standing rules for the use of force (SRUF).[16]

Currently, DoD policy requires that U.S. forces comply with the "fundamental principles and rules" of the law of war during all military operations, not just during armed conflicts.[17] To facilitate that policy, Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3121.01B, on the standing rules governing engagement and the use of force for U.S. forces provides guidance for all DoD operations worldwide and incorporates the law of war.[18] It lays out two frameworks for the use of force during DoD operations, the SRUF and the standing rules of engagement (SROE).[19] Doctrinally, the two frameworks are applicable to distinct mission sets. The SRUF apply to all operations inside U.S. territory, force protection, and security operations at all DoD installations worldwide and to missions performing official security functions off installations abroad, for example, during convoy security operations or bilateral exercises.[20] The SROE apply to all other DoD missions outside

---

[15] This paper only proposes to apply rules for the use of force (RUF) to FDR missions when conducted in predominantly permissive environments, not when natural disasters occur in areas where armed conflict is already taking place or erupts. Here, a permissive environment is defined as one in which the host nation has control and some intent and capability to assist operations. JOINT CHIEFS OF STAFF, JOINT PUB. 3-0, JOINT OPERATIONS, at GL-14 (17 Jan. 2017) (C1 22 Oct. 2018) [hereinafter JP 3-0]. JOINT CAMPAIGNS AND OPERATIONS, at GL-13 (18 June 2022) (defining "permissive environment" as "[u]ncontested conditions in which joint forces have freedom of movement").

[16] This change will require updating JP 3-29, *supra* note 14, and CHAIRMAN, JOINT CHIEFS OF STAFF, INSTR. 3121.01B, STANDING RULES OF ENGAGEMENT/STANDING RULES FOR THE USE OF FORCE FOR U.S. FORCES (13 June 2005).

[17] U.S. DEP'T OF DEF., DIR. 2311.01, DOD LAW OF WAR PROGRAM para. 1.2.a. (2 July 2020).

[18] CHAIRMAN, JOINT CHIEFS OF STAFF, INSTR. 3121.01B, STANDING RULES OF ENGAGEMENT/STANDING RULES FOR THE USE OF FORCE FOR U.S. FORCES (13 June 2005) [hereinafter CJCSI 3121.01B].

[19] *Id.* paras. 3.a.–3.b.

[20] *Id.*

U.S. territory.[21] In accordance with joint doctrine, the SROE apply to humanitarian missions, including FDR.[22]

How to regulate the use of force is a vital decision for the commander of any military operation that requires a careful analysis of how it affects the three levels of warfare: strategic, operational, and tactical.[23] This is no less true when planning FDR missions. Strategically, how is the mission contributing to the DoD's big-picture objectives for providing FDR?[24] Operationally, how is the use of tactical forces linked with those strategic goals?[25] And tactically, do the guidelines for using force give subordinate commanders the tools they need to protect the force and execute the mission?[26]

This paper begins by evaluating why it is important to get the FDR mission right, focusing on the strategic goals and benefits of providing FDR. The next section explores historic FDR missions in Nicaragua and Haiti to demonstrate how ROE was ill-suited to the mission, and how the SRUF could have been a better framework for commanders at the operational and tactical levels. Finally, this paper justifies how RUF are more compatible with the DoD's objectives and obligations when providing FDR.

III. Why It Is Important to Get the FDR Mission Right

To establish the strategic-level value of providing FDR successfully, this section begins by briefly reviewing the domestic law, policy, and guidance governing FDR and how they support the U.S. foreign policy goals of providing aid. Next, it will discuss international norms in the provision of humanitarian aid and how they affect DoD strategic goals. Finally, it shows why FDR is a particularly important mission for the United States right now by discussing how climate change–related disaster compromises national security and how providing FDR will mitigate disaster-related instability and strengthen relationships.

---

[21] *Id.*
[22] JP 3-29, *supra* note 14, at IV-18.
[23] JP 3-0, *supra* note 15, at I-10.
[24] *See* JP 3-0, *supra* note 15, at I-11.
[25] *See* JP 3-0, *supra* note 15, at I-11.
[26] *See* JP 3-0 *supra* note 15, at. at I-11-12.

A. United States' Goal for FDR as Expressed in U.S. Law, Policy, and Guidance

This section highlights that the stated goal for USG intervention in disaster abroad is saving lives and relieving suffering. Then, it argues that the guidance recommending the use of SROE to develop rules to govern the use of force during FDR missions is not optimally suited to achieve that goal.

Legislation, executive orders, and the policy and guidance of both the DoD and the Department of State (DoS) all reiterate the goal of saving lives and relieving suffering when the USG provides disaster assistance abroad. The law governing how and why the USG provides international disaster assistance in natural or man-made disasters is The Foreign Assistance Act of 1961 (FAA).[27] The purpose for providing international disaster assistance in the FAA is to demonstrate "the humanitarian concern and tradition of the people of the United States" by providing "prompt United States assistance to alleviate human suffering caused by natural and manmade disasters."[28]

The U.S. Code and implementing executive order place the DoD in a supporting role to the DoS and U.S. Agency for International Development (USAID) in most humanitarian aid missions.[29] The DoD's speed, specialization, and efficiency are particularly in-demand traits when the barriers to saving lives and relieving human suffering are complex. [30] Leaders responding in FDR missions must ground their

---

[27] Foreign Assistance Act, 22 U.S.C. § 2151–2431. The Foreign Assistance Act (FAA) reorganized the way the USG provides foreign assistance and created the United States Agency for International Development (USAID) to bring multiple government programs and efforts under one agency. *USAID History*, USAID (Nov. 12, 2021), https://www.usaid.gov/who-we-are/usaid-history.

[28] 22 U.S.C. § 2292(a).

[29] *Id.*; Exec. Order No. 12,966, 60 Fed. Reg. 36,949 (July 14, 1995). The FAA grants the President broad authority to respond to foreign disasters, as well as to assist in disaster preparedness, prediction, and planning. 22 U.S.C. § 491. The President then delegates the FAA presidential functions to the Secretary of State, requiring consultation with the Administrator of USAID and/or the SecDef when necessary. Exec. Order No. 12,966, 60 Fed. Reg. 36,949 (July 14, 1995).

[30] STEPHEN DYCUS ET AL., NATIONAL SECURITY LAW 467 (7th ed. 2020). Congress specifically authorizes the DoD to participate in foreign disaster assistance in 10 U.S.C. § 404, which outlines circumstances that may allow the DoD to aid outside the U.S. The President can direct the SecDef to provide foreign disaster assistance "when necessary to prevent loss of lives or serious harm to the environment." 10 U.S.C. § 404. Executive Order 12966, the implementing order for Section 404, grants the SecDef the power to make a

decisions in the fact that the DoD is in a supporting role and that the primary goal is to save lives and relieve the suffering of foreign disaster victims.[31] This fits within the broader DoD goal of providing humanitarian assistance globally.[32] However, joint doctrine recommends the use of the SROE to develop guidance for the use of force in FDR missions.[33]

---

unilateral decision to provide disaster assistance but only in emergency situations if it is necessary to save human lives, and when there is not time to get the concurrence of the Secretary of State. Exec. Order No. 12,966, 60 Fed. Reg. 36,949 (July 14, 1995). Otherwise, the SecDef may only provide disaster assistance at the direction of the President or with the concurrence of the Secretary of State. *Id.* Additionally, 10 U.S.C. § 2561 is an alternate authority that allows the DoD to expend funds for humanitarian assistance. The statute authorizes spending for the transportation of humanitarian relief and "other humanitarian purposes worldwide," a broad clause that can encompass many FDR activities. 10 U.S.C. § 2561. While Section 404 allows the DoD to perform a broad range of FDR missions, it also contains strict reporting requirements, so it may not be the favored authority in emergency situations. DEF. SEC. COOP. AGENCY, U.S. DEP'T OF DEF., SECURITY ASSISTANCE MANAGEMENT MANUAL para. C12.2.7.5 (30 Apr. 2012) [hereinafter SAMM]; *see also* NAT'L SEC. L. DEP'T, THE JUDGE ADVOC. GEN.'S LEGAL CTR. & SCH., U.S. ARMY, OPERATIONAL LAW HANDBOOK 296 (2021) [hereinafter OPERATIONAL LAW HANDBOOK]. Reporting for Section 2561 activities is rolled into the annual Humanitarian Assistance Report to Congress; therefore, the DoD generally performs FDR missions under this authority. The DoD submits activities authorized under Section 2561 annually as a part of the Humanitarian Assistance report to Congress. SAMM, *supra*, para.C12.2.7.2.

[31] JP 3-29 *supra* note 14, at I-1 (defining FDR as "assistance that can be used immediately to alleviate the suffering of foreign disaster victims"). The U.S. Agency for International Development (USAID) only requests DoD support in about 10 percent of USG responses to foreign disasters. OPERATIONAL LAW HANDBOOK, *supra* note 30, at 290.

[32] The Secretary of Defense (SECDEF) laid out goals for humanitarian programs using the Overseas Humanitarian, Disaster, and Civic Aid Appropriation as follows:

> [C]onsistent with references b through e, and to the extent permitted by law, the DoD HA program will be used to promote the following objectives globally: (1) improve the basic living conditions of the civilian populace in a country or region that is susceptible to violent extremism and/or is otherwise strategically important to the United States; (2) enhance the legitimacy of the HN by improving its capacity to provide essential services to its populace; (3) promote interoperability and coalition-building with foreign military and civilian counterparts; (4) generate long-term positive perceptions of DoD and the USG with HN civilian and military institutions; and (5) enhance security and promote enduring stability in the HN or region.

Memorandum from Assistant Sec'y of Def. for Special Operations and Low Intensity Conflict, subject: Policy Guidance for DOD Humanitarian Assistance Funded by the Overseas Humanitarian, Disaster, And Civic Aid Appropriation para. 3(c) (5 June 2012).

[33] JP 3-29, *supra* note 14, at IV-18. United States joint doctrine is official advice meant to guide the commanders of the joint force in pursuit of shared goals and generally does not

The DoS Foreign Affairs Manual on International Disaster and Foreign Assistance states in its general policy that "the United States may provide humanitarian assistance to affected populations."[34] The primary DoS goal when providing refugee and humanitarian assistance is saving lives and relieving human suffering.[35] Thus, the DoD and DoS agree on the goal in FDR: saving lives and relieving suffering.

The next section will evaluate international norms and expectations. As stated in the FAA, part of the purpose of humanitarian missions is to "demonstrate the humanitarian concern and tradition of the people of the United States" [36] and using RUF will better express that to the global audience.

B. International Norms and Expectations

Rules of engagement logically apply when host-nation law enforcement is ineffective or hostile to U.S. forces.[37] In the humanitarian context, the host nation generally retains primary responsibility for law enforcement, including protecting the victims of the disaster.[38] Outside of armed conflict, there is no international justification for supplanting the local military/law enforcement role without host-nation consent. Therefore, when deployed on FDR missions, the DoD must comply with host-nation law and international obligations, rely on a status of forces agreement (SOFA), or assume risk.[39]

The United Nations (U.N.) General Assembly approved guiding principles for "strengthening the coordination of humanitarian emergency assistance" in 1991.[40] Among those principles is that assistance "must be provided in accordance with the principles of humanity, neutrality, and

---

establish policy. JOINT CHIEFS OF STAFF, JOINT PUB. 1, DOCTRINE FOR THE ARMED FORCES OF THE UNITED STATES, at I-1 (25 Mar. 2013) (C1 12 July 2017).

[34] 2 U.S. DEP'T OF STATE, FOREIGN AFFAIRS MANUAL para. 061 (2022) [hereinafter DoS FAM].

[35] *Id.* para. 061.2; *Refugee and Humanitarian Assistance*, U.S. DEP'T OF STATE, https://www.state.gov/policy-issues/refugee-and-humanitarian-assistance (last visited Apr. 11, 2023).

[36] 22 U.S.C. § 2292(a).

[37] *See* CTR. FOR L. & MIL. OPERATIONS, THE JUDGE ADVOC. GEN.'S LEGAL CTR. & SCH., U.S. ARMY & INT'L & OPERATIONAL L. BRANCH, JUDGE ADVOC. DIV., U.S. MARINE CORPS, ROE v. RUF [hereinafter ROE v. RUF].

[38] DoS FAM *supra* note 34. This would not be the case in situations where disaster strikes areas already involved in armed conflict.

[39] *See generally* U.N. Charter art. 2.

[40] G.A. Res. 46/182, ¶ 50 (Dec. 19, 1991).

impartiality" and "[s]overeignty, territorial integrity and national unity of States must be fully respected."[41] There is no exemption to sovereignty for providing humanitarian aid after a disaster; the USG needs the consent of the affected country to fulfill its mission.[42]

United Nations General Assembly Resolution 58/114 reaffirms these guiding principles and elaborates on the role of the military in humanitarian efforts.[43] It emphasizes that humanitarian assistance is a civilian-led process and affirms that when military forces are used, their use should respect humanitarian law and principles.[44] It notes that the Oslo Guidelines can inform the use of force in humanitarian relief efforts.[45]

The Oslo Guidelines are nonbinding guidance published by the U.N. Office for the Coordination of Humanitarian Affairs to "formaliz[e] and improv[e] the effectiveness and efficiency of the use of foreign military and civil defence assets in international disaster relief efforts."[46] The U.S. military has incorporated the guidelines into doctrine in JP 3-29.[47] The Oslo Guidelines elaborate on the General Assembly Resolution guiding principles of sovereignty, territorial integrity, and national unity, including and defining the principles of humanity, neutrality, and impartiality.[48] They prohibit as a matter of principle the use of military forces actively engaged in combat to support humanitarian operations.[49] When military assets are used to support humanitarian operations, the overall mission "must retain its civilian nature and character."[50] The host nation has primary responsibility for security.[51]

The international community may be skeptical of the use of militaries in humanitarian contexts. Thus, the USG may need to negotiate force protection and force posture with the host nation when providing aid.[52] The U.N. Guidelines on the *Use of Military and Civil Defence Assets to*

---

[41] *Id.*
[42] Office for the Coordination of Humanitarian Affairs, Guidelines on the Use of Foreign Military and Civil Defence Assets in Disaster Relief, para. 21, U.N. Doc. OCHA/ESB/2008/6 (Nov. 1, 2007) [hereinafter Oslo Guidelines].
[43] G. A. Res. 58/114, ¶ 9 (Dec. 17, 2003).
[44] *Id.*
[45] *Id.*
[46] Oslo Guidelines *supra* note 42, para. 16.
[47] Lieutenant Colonel John N. Ohlweiler, *Building the Airplane While in Flight: International and Military Law Challenges in Operation Unified Response*, ARMY LAW. Jan. 2011, at 9, 14. *See also* JP 3-29 *supra* note 14, at III-7.
[48] *See* Oslo Guidelines *supra* note 42, para. 20.
[49] Oslo Guidelines *supra* note 42, para. 23.
[50] Oslo Guidelines *supra* note 42, para. 32.iii.
[51] Oslo Guidelines *supra* note 42, para. 29.
[52] *See infra* Section IV.A. (explaining negotiations with the government of Nicaragua during Operation Fuerte Apoyo).

Support United Nations Humanitarian Activities in Complex Emergencies warn that the use of force can "compromise neutrality, impartiality, and other humanitarian principles." [53] Losing neutrality can result in belligerents denying relief workers' access to affected areas or targeting the affected population directly. This problem can go on for years and affect future disaster relief operations.[54] The U.N. also sees foreign forces under the authority of their own government, rather than under the U.N. mission, as potentially problematic on humanitarian missions. [55] The military may have other motivations, like to "legitimize missions, gain intelligence and or enhance protection of forces." [56] Demonstrating a commitment to human rights, avoiding unnecessary use of force and distinguishing the mission from combat operations, may relieve any skepticism towards the DoD assisting USG efforts in FDR.

The next section will explain that climate change is a developing threat to U.S. national security and a stable international order. As disasters mount and compound, the need for effective help will only grow among U.S. partner nations. Doing more FDR missions may increase the risk that U.S. competitors seize on a mistake and use it against U.S. interests.

C. Climate Change and Its National Security Impact

Over the last century, the United States has developed a reputation as a world leader in the provision of FDR.[57] The USG does this partially as a demonstration of goodwill and solidarity with states who are victims of disaster, but also to promote security, stability, reduce conflict, and expand democracy and free markets.[58] As climate change creates unpredictable weather patterns, the number of complex and acute disasters that require the USG to call in the DoD for assistance will increase. If the United States is going to contribute to more FDR missions in the near future, it increases the chance that unnecessary use of force will derail the strategic goals of saving lives and relieving suffering to demonstrate good will.

---

[53] U.N. Off. for the Coordination of Humanitarian Aff., Guidelines on the Use of Military and Civil Defence Assets to Support United Nations Humanitarian Activities in Complex Emergencies, para. 32 (2006).
[54] *Id.*
[55] *Id.* para. 35.
[56] *Id.*
[57] *See* Julia F. Irwin, *The Origins of U.S. Foreign Disaster Assistance*, AM. HISTORIAN, Feb. 2018, at 43–49.
[58] *USAID History*, *supra* note 27.

The 2021 *DoD Climate Risk Analysis* finds that climate change is increasing the number and severity of extreme-weather-related disasters, and "impacts are likely to expand competition over regions and resources, affect the demands on and functionality of military operations, and increase the number and severity of humanitarian crises, at times threatening stability and security."[59] The analysis specifically notes the security implications of climate change in the Indo-Pacific, and how "competitors such as China may try to take advantage of climate change impacts to gain influence."[60]

China has aggressively pursued relationships with small countries in South and Southeast Asia to gain influence and military advantage.[61] The Philippines ranked fourth on the Long-Term Climate Risk Index, which tracked the countries most affected by climate change from 2000–2019.[62] In fact, six of the top ten nations on the Climate Risk Index are in South or Southeast Asia, and climate-change-related disaster in that region could have a serious impact on U.S. national security.[63] If the DoD takes an active support role and an injudicious use of force occurs, it provides fuel that U.S. regional competitors can use. China is known to "exploit the conditions of the operational environment to achieve their objectives without resorting to armed conflict by fracturing the U.S.'s alliances, partnerships, and resolve."[64] United States policy should guard against the risk of that exploitation.

Getting the FDR mission right means the primary goal is to save lives and relieve human suffering. This is the mandate of U.S. domestic rules and foreign policy goals governing FDR. International norms and expectations emphasize these goals but balance them with the sovereignty and dignity of the nations that need aid. And the looming threat of climate change–related disaster means that there will be more opportunities to fail and risk the stable world order the USG works to build and preserve. The next section will introduce case studies that illustrate how the DoD has worked in the past to fulfill the goals and mission of FDR, and how using ROE did not optimally support that effort.

---

[59] U.S. DEP'T OF DEF., DEPARTMENT OF DEFENSE CLIMATE RISK ANALYSIS 8 (2021).
[60] *Id.* at 6.
[61] *See* JOSHUA T. WHITE, BROOKINGS INST., CHINA'S INDIAN OCEAN AMBITIONS: INVESTMENT, INFLUENCE, AND MILITARY ADVANTAGE (2020); MADIHA AFZAL, BROOKINGS INST., "AT ALL COSTS": HOW PAKISTAN AND CHINA CONTROL THE NARRATIVE ON THE CHINA-PAKISTAN ECONOMIC CORRIDOR (2020).
[62] GCRI 2021, *supra* note 1, tbl. 2.
[63] *See infra* Appendix B; WHITE, *supra* note 61; AFZAL, *supra* note 61.
[64] U.S. DEP'T OF THE ARMY, TRADOC PAM. 525-3-1, THE U.S. ARMY IN MULTI-DOMAIN OPERATIONS 2028 para. 2b (6 Dec. 2018).

IV. Case Studies

This section will explore two major disaster relief operations that took place in the last twenty-five years, Operation Fuerte Apoyo and Operation Unified Response. Each illustrates why the SROE is not the optimal tool for regulating the use of force in operations. Operation Fuerte Apoyo focused on providing relief to the thousands of people suffering from the effects of Hurricane Mitch in Central America in 1998.[65] During this operation, particularly in Nicaragua, commanders had trouble balancing force protection with public affairs and the need to demonstrate to the local population and the world at large that the purpose of the military presence was to relieve human suffering.[66] Operation Unified Response responded to a massive earthquake that devastated Haiti in 2010.[67] It was one of the largest deployments of U.S. forces for disaster relief, combining and amplifying the delicate issues faced by commanders in Central America.[68] Additionally, this section demonstrates the challenges of molding ROE for a situation where identified threats may also be the victims the USG intends to assist.

A. Operation Fuerte Apoyo: Central America, 1998

Hurricane Mitch struck at a terrible time for Central America. Following the 1997–1998 El Niño pattern, the nations occupying the isthmus between Mexico and South America were already struggling to recover from floods, droughts, and wildfires caused by extreme weather.[69] Hurricane Mitch formed as a Category 5 hurricane over the Caribbean Sea, but by the time it struck Honduras, it was only a Category 1 storm.[70] However, once it hit land on 30 October 1998, it stopped moving and

---

[65] *See* CTR. FOR L. & MIL. OPERATIONS, THE JUDGE ADVOC. GEN.'S LEGAL CTR. & SCH., U.S. ARMY, LAW AND MILITARY OPERATIONS IN CENTRAL AMERICA: HURRICANE MITCH RELIEF EFFORTS, 1998–1999 LESSONS LEARNED FOR JUDGE ADVOCATES 8 (2000) [hereinafter HURRICANE MITCH RELIEF EFFORTS].

[66] *See id.* at 64-65.

[67] GARY CECCHINE ET AL., THE U.S. MILITARY RESPONSE TO THE 2010 HAITI EARTHQUAKE: CONSIDERATIONS FOR ARMY LEADERS 1-4 (2013).

[68] *See id.* at 31.

[69] Pan Am. Health Org., *Impact of Hurricane Mitch in Central America*, EPIDEMIOLOGICAL BULL., Dec. 1998, at 1, 1 [hereinafter PAHO].

[70] JOHN L. GUINEY & MILES B. LAWRENCE, NAT'L OCEANIC AND ATMOSPHERIC ADMIN., PRELIMINARY REPORT, HURRICANE MITCH, 22 OCTOBER–05 NOVEMBER 1998, at 2 (1999).

inundated the region with rain for four days.[71] The extreme rainfall washed out bridges and destroyed roads, homes, hospitals, and other vital infrastructure.[72] To this day, experts consider Hurricane Mitch the deadliest hurricane in the last 200 years, causing over 9,000 deaths in the region.[73] It caused widespread food insecurity, lack of access to drinking water and public health resources, and severely damaged the infrastructure necessary to bring help to the victims.[74] Honduras suffered the most extensive damage from the storm, with significant damage also occurring in Nicaragua, El Salvador, Guatemala, and some damage in Costa Rica.[75]

The DoD was able to respond to Hurricane Mitch swiftly, primarily because there was already a joint task force (JTF-BRAVO) based at Soto Cano Airbase in Honduras.[76] Before the hurricane hit land, JTF-BRAVO prepared to act as an intermediate staging base.[77] The chief of mission (COM) in Honduras declared a disaster, freeing up disaster relief funding.[78] On 4 November 1998, the Joint Chiefs of Staff issued a deployment order in response to a request for support from U.S. Southern Command (USSOUTHCOM) for disaster relief operations.[79] The next day, the U.S. President directed that the DoD provide up to $30 million in support to the mission.[80]

Judge advocates (JAs) deployed in support of Operation Fuerte Apoyo reported that force-protection issues were a focus of their efforts during the initial emergency relief phase and through the rehabilitation and restoration phases of the operation.[81] The area of responsibility (AOR) had a high crime rate, even before the emergency.[82] Furthermore, in Nicaragua, JAs perceived an anti-U.S. sentiment among the locals based on U.S. support to the Contras in the 1980s.[83] The Joint Task Force (JTF) commander classified force protection as the number one priority of the task force, and said "nothing we do is worth serious injury or the loss of

---

[71] HURRICANE MITCH RELIEF EFFORTS, *supra* note 65, at 1-4.
[72] HURRICANE MITCH RELIEF EFFORTS, *supra* note 65, at 1-4.
[73] GUINEY & LAWRENCE, *supra* note 70, at 1; PAHO, *supra* note 69, at 2 tbl.1.
[74] PAHO, *supra* note 69, at 4-5.
[75] *See* PAHO, *supra* note 69, at 2 tbl.1.
[76] HURRICANE MITCH RELIEF EFFORTS, *supra* note 65, at 5.
[77] HURRICANE MITCH RELIEF EFFORTS, *supra* note 65, at 5.
[78] HURRICANE MITCH RELIEF EFFORTS, *supra* note 65, at 5.
[79] A. MARTIN LIDY ET AL., INST. FOR DEF. ANALYSES, EFFECTIVENESS OF DOD HUMANITARIAN RELIEF EFFORTS IN RESPONSE TO HURRICANES GEORGES AND MITCH, ES-7 (2001). The National command authority approved USSOUTHCOM's request. *Id.*
[80] HURRICANE MITCH RELIEF EFFORTS, *supra* note 65, at 8.
[81] HURRICANE MITCH RELIEF EFFORTS, *supra* note 65, at 35.
[82] HURRICANE MITCH RELIEF EFFORTS, *supra* note 65, at 97.
[83] HURRICANE MITCH RELIEF EFFORTS, *supra* note 65, at 97.

life."[84] However, commanders also found that force protection did not necessarily require the use of force. For example, commanders found success using information operations and public affairs strategies to improve safety.[85] The force protection condition (FPCON) for the mission was ALPHA+, including security measures like limiting access and coordinating with the COM and local government about terrorist activity, but stopping short of naming any hostile group or advising any offensive security missions.[86] Rather, planning focused on force protection similar to that allowed by the SRUF.[87] Commanders cancelled missions in areas where confrontations were likely and the threat was high.[88] While FPCON ALPHA+ lists the potential for possible terrorist activity against protected persons and objects, it puts in place measures that will allow the command to protect the force.[89] All of these force protection measures short of the use of force are permissible under ROE; the SROE does not mandate any use of force.[90] However, the measures used here are an excellent example of how commanders would ensure force protection under the SRUF if the use of force is more restricted in a particular case.

Soldiers operated under ROE in Operation Fuerte Apoyo.[91] Leaders in the 82d Airborne Division had already trained their paratroopers on the basics of ROE.[92] Then, leaders in theater provided additional training to incorporate the USSOUTHCOM ROE and issued USSOUTHCOM ROE cards when the paratroopers arrived.[93] However, due to the lack of a SOFA, the USG negotiated the status of forces with Nicaragua as forces

---

[84] Memorandum from Commander, Joint Task Force Aguila, subject: Policy Letter #4, Force Protection (3 Jan. 1999), *in* CTR. FOR L. & MIL. OPERATIONS, THE JUDGE ADVOC. GEN.'S LEGAL CTR. & SCH., U.S. ARMY, LAW AND MILITARY OPERATIONS IN CENTRAL AMERICA: HURRICANE MITCH RELIEF EFFORTS, 1998–1999, app. E-1 (15 Sept. 2000) [hereinafter Pol'y Letter 4].

[85] *Id.* at 118; *see also* LIDY ET AL., *supra* note 79, at II.18.

[86] Pol'y Letter 4, *supra* note 84, encl. 2.

[87] Pol'y Letter 4, *supra* note 84, encl. 2. Force protection condition (FPCON) was formerly known by the acronym THREATCON and is listed as such in this reference. U.S. DEP'T OF DEF., INSTR. 2000.16, TERRORIST THREAT CONDITION encl. 3, para. E3.1.1.7.2 (14 June 2001).

[88] HURRICANE MITCH RELIEF EFFORTS, *supra* note 65, at 97.

[89] Pol'y Letter 4, *supra* note 84, encl. 2, para. c.

[90] *See generally* CJCSI 3121.01B *supra* note 18.

[91] Commander, Joint Task Force Aguila, Gen. Order No. 1 (Dec. 6 1998) *in* CTR. FOR L. & MIL. OPERATIONS, THE JUDGE ADVOC. GEN.'S LEGAL CTR. & SCH., U.S. ARMY, LAW AND MILITARY OPERATIONS IN CENTRAL AMERICA: HURRICANE MITCH RELIEF EFFORTS, 1998–1999, app. J-4 (15 Sep. 2000).

[92] HURRICANE MITCH RELIEF EFFORTS, *supra* note 65, at 99.

[93] HURRICANE MITCH RELIEF EFFORTS, *supra* note 65, at 99.

deployed, likely making some of that ROE training and ROE development incomplete.[94]

Negotiators did not reach agreement on a SOFA; instead, an exchange of diplomatic notes covered some of the issues relevant to the status of U.S. personnel.[95] However, the diplomatic notes did not contain the typical language allowing Soldiers to carry weapons for self-defense.[96] This was due to an objection by the Nicaraguan government to the "possible perception of such language" by the Nicaraguan population.[97] Nicaraguan leaders did not want the perception that U.S. forces were occupying territory; commanders had to take this into account when determining how best to provide for subordinate commanders' right and obligation to exercise unit self-defense.[98] United States forces operated under an unspoken understanding and carried weapons discretely.[99] For example, engineers were limited to carrying sidearms rather than traveling in vehicles with large weapons mounted.[100]

A study by the Institute for Defense Analyses examined the response to Hurricane Mitch to evaluate the U.S. capacity to provide humanitarian assistance following natural disasters.[101] Evaluating the force protection requirements, the authors of the study found that stringent force protection measures impeded forces' ability to conduct humanitarian missions, and recommended that in future efforts, commanders consider less-strict force protection measures in what they call a "non-conflictive" environment.[102] These may include allowing missions to take place with less coordination of movement, lower approval levels, and fewer force protection personnel.[103]

The analysis also notes that "large-scale natural disasters such as Hurricane Mitch have major political implications" and that commanders "confronted operational decisions with significant political implications within the host countries."[104] Failure to address those issues appropriately "could have led to foreign policy or media relations difficulties, complicating the primary mission: meeting the relief needs of storm

---

[94] *See* LIDY ET AL., *supra* note 79, at B-104.
[95] LIDY ET AL., *supra* note 79, at B-104.
[96] HURRICANE MITCH RELIEF EFFORTS *supra* note 65, at 64–65.
[97] HURRICANE MITCH RELIEF EFFORTS *supra* note 65, at 64–65.
[98] *See* LIDY ET AL., *supra* note 79, at B-91.
[99] HURRICANE MITCH RELIEF EFFORTS, *supra* note 65, at 64.
[100] HURRICANE MITCH RELIEF EFFORTS, *supra* note 65, at 64.
[101] *See* LIDY ET AL, *supra* note 79.
[102] LIDY ET AL., *supra* note 79, at B-92.
[103] LIDY ET AL., *supra* note 79, at B-91.
[104] LIDY ET AL., *supra* note 79, at B-48.

victims."[105] While the discussion does not specifically lay out the ROE as an example of these decisions, it does point out sensitivities to carrying arms openly and interacting with the local population.

B. Operation Unified Response: Haiti, 2010

Twelve years after Hurricane Mitch, another disaster struck in the USSOUTHCOM AOR, this time in the form of a massive 7.0 earthquake centered near Port-au-Prince, Haiti, on 12 January 2010.[106] Estimates show that the earthquake and resulting chaos killed over 230,000 people, injured 300,000, and displaced more than 1.5 million in a nation of nearly 10 million.[107] In Haiti, like in Nicaragua, the United States had a history of intervention in Haitian politics, sending troops in 1915 to protect American interests in Haiti during a period of extreme political unrest and again in 1994 to support the presidency of Jean-Bertrand Aristide.[108] In the aftermath of the earthquake, U.S. President Barack Obama directed the USG to "respond with a swift, coordinated, and aggressive effort to save lives," and the DoD complied.[109] What followed was "the U.S. military's largest international humanitarian effort in history."[110]

By chance, the deputy commanding general of USSOUTHCOM, Lieutenant General (LTG) P.K. Keen was on the ground in Haiti on the day of the earthquake, and swiftly assumed leadership of the newly formed Joint Task Force-Haiti (JTF-H).[111] This task force leapt into action, relying heavily on verbal orders from LTG Keen to request forces and supplies swiftly and efficiently.[112] In doing so, the JTF-H planners sidestepped some policy procedures, like coordinating force personnel as they flowed into the AOR.[113]

The DoD assembled a joint force including an assault command post from XVIII Airborne Corps, an Air Force squadron to reestablish

---

[105] LIDY ET AL., *supra* note 79, at B-48.
[106] DEBARATI GUHA-SAPIR ET AL., U.S. AGENCY FOR INT'L DEV., INDEPENDENT REVIEW OF THE U.S. GOVERNMENT RESPONSE TO THE HAITI EARTHQUAKE 17 (2011).
[107] *Id.*
[108] Ohlweiler *supra* note 47, at 11–12.
[109] *Obama Vows Unwavering Support for Quake-Hit Haiti*, REUTERS (Jan. 13, 2021, 10:35 am), https://www.reuters.com/article/us-quake-haiti-obama-statement/obama-vows-unwavering-support-for-quake-hit-haiti-idUSTRE60C3PW20100113.
[110] CECCHINE, *supra* note 67, at 31.
[111] CECCHINE, *supra* note 67, at 4.
[112] *See* CECCHINE, *supra* note 67, at 34.
[113] GUHA-SAPIR ET AL., *supra* note 106,106 at 47.

operations at the airport, U.S. Coast Guard cutters, U.S. Navy ships, and Special Forces teams, all within only three days of the emergency and all falling under the operational authority of LTG Keen and JTF-H.[114] Collecting the forces to serve in the JTF was a complex undertaking.[115] Units selected for deployment were scattered across the country, from the active and Reserve components, at varying readiness and mobilization states, and all of their deployments had to be coordinated as quickly as possible.[116] At one point, over 22,200 people worked for JTF-H.[117]

Since 2004, the U.N. Stabilization Mission in Haiti (MINUSTAH) operated as a combined military force to stabilize the nation, following extensive armed conflict in the country that had resulted in a military coup.[118] Tragically, the MINUSTAH headquarters building collapsed during the earthquake, killing the head of mission and his principal deputy along with dozens of MINUSTAH staff.[119] Following the earthquake, MINUSTAH was authorized higher force levels to "support the immediate recovery, reconstruction and stability efforts in the country."[120] One of their missions was to "protect U.N. personnel, facilities, installations, and equipment, and protect civilians under imminent threat of physical violence."[121] This mission belonged to MINUSTAH, and was not a U.S. authority or mission in Haiti, other than those U.S. forces specifically assigned to MINUSTAH.[122]

The world community did not universally respond positively to the large-scale U.S. response. Even France, a strong ally, felt like the United States was disproportionately involved in the relief operation.[123] Some leaders from Latin America, including the president of Nicaragua, and other more typical dissenting voices like the President of Cuba, voiced suspicions that it was a U.S. military occupation of Haiti rather than a targeted relief mission.[124] Hugo Chavez, then-President of Venezuela, suggested that it was a military occupation and that U.S. weapons testing

---

[114] *See* CECCHINE, *supra* note 67, at 33 fig.3.1.
[115] *See* DAVID R. DIORIO, OPERATION UNIFIED RESPONSE – HAITI EARTHQUAKE 2010, at 8 (2010).
[116] *See id.*
[117] CECCHINE, *supra* note 67, at 40.
[118] *See MINUSTAH Fact Sheet*, U.N. PEACEKEEPING, https://peacekeeping.un.org/en/mission/minustah (last visited May 3, 2023).
[119] CECCHINE, *supra* note 67, at 1.
[120] *MINUSTAH Fact Sheet*, *supra* note 118.
[121] CECCHINE, *supra* note 67, at 53.
[122] CECCHINE, *supra* note 67, at 55.
[123] DIORIO, *supra* note 115, at 3.
[124] DIORIO, *supra* note 115, at 3.

caused the earthquake.[125] Partially to combat these rumors, the U.N. brokered an agreement wherein MINUSTAH continued its mission to conduct security and stability operations in the country, and JTF-H focused its attention on providing humanitarian assistance and disaster relief and maintained responsibility for the required ports, airports, and roads to transport supplies.[126] Joint Task Force-Haiti honed its communications to demonstrate to key audiences that the USG was part of a global effort to help and not an occupying force.[127]

The USSOUTHCOM Office of Strategic Communications worked hard on strategic communications.[128] Joseph "Pepper" Bryars of that office recommended transparency, including sharing intelligence and rules of engagement.[129] He noted that the U.S. role in providing security in the area was subject to interpretation, and the Haitian, U.S., and international audiences would scrutinize any use of force, and, therefore, strategic communications needed to manage messaging on that mission.[130] One method he recommended was demonstrating a "unified face," always focusing on showing JTF-H personnel working with or for USG civilians, not undertaking exclusive military missions.[131]

Violence levels were low in the immediate aftermath of the earthquake, despite delays in distributing relief, lack of local police, and the release of approximately four thousand inmates from a Port-au-Prince prison.[132] However, as vital supplies dwindled, violence broke out across the country.[133] The European Union deployed 300–350 police officers to aid in providing security to protect convoys and supplies.[134]

In the midst of this organized chaos, JAs were responsible for assisting the command in developing rules of engagement for the operation based on the SROE.[135] The deputy staff judge advocate for JTF-H during the first few months of the relief effort was Lieutenant Colonel John N. Ohlweiler.[136] During his time in Haiti, he identified two principal

---

[125] John "Jay" Boyd, *The Pitfalls of Well-Meaning Compassion Joint Task Force-Haiti's Infowar of 2010*, MIL. REV., Jan.-Feb. 2021, at 108, 114; CECCHINE, *supra* note 67, at 3.
[126] CECCHINE, *supra* note 67, at 4–5; DIORIO, *supra* note 115, at 3.
[127] DIORIO, *supra* note 115, at 14.
[128] Boyd, *supra* note 125, at 110.
[129] Boyd, *supra* note 125, at 112.
[130] Boyd, *supra* note 125, at 112.
[131] Boyd, *supra* note 125, at 112.
[132] DIORIO, *supra* note 115, at 1.
[133] DIORIO, *supra* note 115, at 7-8.
[134] DIORIO, *supra* note 115, at 8.
[135] *See* Ohlweiler *supra* note 47, at 10, 15.
[136] Ohlweiler *supra* note 47, at 9.

challenges in developing ROE for the combat-tested force: recalibrating the purpose and effect of escalation of force (EOF) procedures for a humanitarian mission and identifying specific property that forces could protect with deadly force.[137]

Traditionally, EOF was a method of assessing and possibly subduing threats identified by Service members.[138] During training and combat engagements in the Iraq and Afghanistan theaters over the previous nine years, EOF procedures became a tool of assessing threats and determining hostile intent prior to engaging with lethal force.[139] This subtle shift changed the mentality of Service members approaching civilians. Rather than assuming civilians were peaceful unless given evidence to the contrary, it trained Service members to see all civilians as a potential threat.[140] The ROE team in Haiti crafted EOF procedures that emphasized evaluating the situation and disengaging before resorting to non-lethal measures when possible.[141]

The commanders developed an ROE that only authorized lethal measures to defend U.S. forces or other designated persons and specifically designated property, including military weapons and some critical infrastructure.[142] After much discussion, the JTF-H commander did not authorize Service members to defend food, water, and supplies, for the simple reason that the people trying to steal those supplies probably were in desperate need of them.[143] This guidance for the use of force incorporates the congressional mission and purpose as well as foreign policy goals. The SRUF can allow for the use of deadly force for self-defense, to protect assets vital to national security, inherently dangerous property, or national critical infrastructure.[144] When directly related to the mission, Service members may be authorized to use it where serious offenses involving the imminent threat of death or serious bodily harm to others occur.[145] Protection of food and supplies are unlikely to fall under any of these categories and are unlikely necessary to relieve suffering and save lives.

This is just one example of how the SRUF better meets congressional and foreign policy goals because it emphasizes restraint. The applicable restraint in the SROE in this case is the law of armed conflict, so a

---

[137] Ohlweiler *supra* note 47, at 15.
[138] Ohlweiler *supra* note 47, at 16.
[139] Ohlweiler *supra* note 47, at 16.
[140] Ohlweiler *supra* note 47, at 16-17.
[141] Ohlweiler *supra* note 47, at 17.
[142] Ohlweiler *supra* note 47, at 18.
[143] Ohlweiler *supra* note 47, at 20.
[144] CJCSI 3121.01B *supra* note 18, encl. L, para. 5.c.
[145] CJCSI 3121.01B *supra* note 18, encl. L, para. 5.c.

commander would be making a necessity and proportionality decision, possibly for every incident.[146] The ROE proportionality analysis has the commander weigh the use of force against what is sufficient to respond decisively to hostile acts or intent at the tactical level.[147] This is inefficient in an FDR mission, where the emphasis is on relieving human suffering and saving lives. Thus, the planners at the operational level would streamline the process if they use the SRUF to achieve strategic goals.

The urgency of the need and the uncertainty of the situation on the ground made the massive verbal-order-driven push of people and supplies into Haiti a bold choice that paid great dividends on the success of the mission; however, there were drawbacks. For example, forces arrived with less training, guidance, and direction than they would have in a normal orders-based process.[148] The JAs in the ROE planning cell were proposing EOF procedures that had never been seen—let alone used—by the vast majority of the force, which likely added to the burden of those JAs training Service members as they deployed to Haiti and the comprehension level of the training audiences.[149] These JAs responsible for training the force were not centrally located and Service members came from both the active and Reserve force, which required exponentially more coordination.

Many of the principles considered by the JTF-H legal team when developing the ROE were already incorporated in the SRUF, including de-escalation procedures and restrictions on the use of lethal force when not in self-defense.[150] Those far-flung JAs could have been looking up the SRUF in their trusty *Operational Law Handbooks* while still at home station preparing their training(s), rather than hoping they were on the right JTF-H listserv to receive a highly mission-specific ROE.[151]

The missions to Nicaragua and Haiti were very successful by most measures. They delivered vital supplies, repaired infrastructure, and fulfilled their primary mission to relieve human suffering.[152] The leaders and JAs who deployed and worked hard to develop and train on ROE should be proud and commended. However, had the SRUF been the

---

[146] *See* OFF. OF GEN. COUNS., U.S. DEP'T OF DEF., DEPARTMENT OF DEFENSE LAW OF WAR MANUAL §§ 2.2, 2.4 (12 June 2015) (C2, 13 Dec. 2016).
[147] CJCSI 3121.01B *supra* note 18, encl. A, para.4.a.(3).
[148] *See* CECCHINE, *supra* note 67, at 40.
[149] *See* Ohlweiler *supra* note 47, at 16-18.
[150] *See* CJCSI 3121.01B *supra* note 18, encl. L, para. 5.
[151] The Judge Advocate Legal Center and School publishes the Operational Law Handbook as a resource for judge advocates in the field practicing national security law. OPERATIONAL LAW HANDBOOK *supra* note 31.
[152] *See* Ohlweiler *supra* note 47; HURRICANE MITCH RELIEF EFFORTS, *supra* note 65, at 10–14.

recommended framework, a lot of the measures forced to fit into ROE, like novel EOF procedures and tortuous force protection measures, may have been developed more easily, allowing leaders to focus on other vital decisions.

The next section will expand on many of the issues brought up in these case studies to show why RUF are better suited for FDR missions. Particularly, it will focus on the protections already contained in the SRUF, the preparation and training of Service members deploying on an FDR mission, and the importance and fragility of public perception and media attention on FDR missions.

V. Why RUF is Better Suited to FDR

Regarding the question at hand—what framework for the use of force should U.S. forces implement during FDR operations—there are at least three answers. The first option is to maintain the status quo and continue to use ROE, adjusting as necessary to suit the mission. The second is to develop a new framework specifically for the use of force during an FDR mission. The third option, and the one embraced by this paper, is to apply RUF, adjusting as necessary to suit the mission.

This section begins to explore those three options by analyzing the salient differences between the SROE and the SRUF. It starts by examining the doctrinal language and then analyzing why those differences are important in deciding which framework to apply to the mission sets. Next, it will discuss how using RUF helps Soldiers succeed by allowing leaders to separate the battlefield mindset from humanitarian missions. It will also discuss the benefit of using a tool that is already in the DoD toolkit: the SRUF. Then, it will discuss the role of public perception and the media in FDR and how RUF help the DoD project the right message about its goal to save lives and relieve human suffering. Finally, it will address how the DoD's focus is changing from counterterrorism/counterinsurgency operations to large-scale combat operations (LSCO), how that may affect the SROE and how they are trained and applied, and why it pulls the SROE even farther from alignment with the goals of FDR.

A. ROE and RUF are Different

Rules of engagement are the commander's tool to regulate the use of force during operations outside the United States, to manage risk, and to

achieve mission success.[153] The rules are highly scalable, but they always provide for a commander's inherent right and obligation to defend the unit against a hostile act or demonstrated hostile intent.[154] The rules can restrict weapons authorized, restrict areas of operation, declare certain forces hostile, and restrict targeting locations among many other options.[155] However, the SROE are largely nonrestrictive; individual commanders can determine if a particular weapon or tactic complies with the law of armed conflict, unless the SROE specifies a higher approval authority or an approved supplemental measure already restricts the use of that weapon or tactic.[156]

While ROE are flexible enough to apply to many different missions, with different levels of risk, doctrinal language generally associates ROE with missions that anticipate conflict. Rules of engagement are defined as "[d]irectives issued by competent military authority that delineate the circumstances and limitations under which United States forces will *initiate and/or continue combat engagement* with other forces encountered."[157] The SROE restate U.S. national security policy "to ensure the survival, safety, and vitality of our [N]ation and to maintain a stable international environment consistent with U.S. national interests."[158] It specifies the objectives of defeating armed attack or terrorist actions against protected persons.[159] The SROE allow commanders to declare a force "hostile," allowing U.S. forces to target them based on their status whether or not they pose an imminent threat of death or serious bodily harm to the unit.[160] Rules of engagement are best suited to engagements that anticipate conflict with hostile actors.

The SRUF bear many similarities to the SROE. They also consistently emphasize a commander's inherent right and obligation to exercise unit self-defense, and include an identical definition of self-defense.[161] However, unlike the SROE, the SRUF are primarily restrictive, so weapons and tactics that the SRUF do not approve require SECDEF

---

[153] *See* CJCSI 3121.01B *supra* note 18, at 1-3. Rules of engagement can also apply to air and maritime forces on homeland defense missions inside the U.S. CJCSI 3121.01B *supra* note 18, para. 3.a.
[154] *See* CJCSI 3121.01B *supra* note 18, at 2.
[155] *See* CJCSI 3121.01B *supra* note 18, at 2-3.
[156] CJCSI 3121.01B *supra* note 18, at 3.
[157] JOINT CHIEFS OF STAFF, JOINT PUB. 1-04, LEGAL SUPPORT TO MILITARY OPERATIONS, at GL-3 (2 Aug. 2016) (emphasis added).
[158] CJCSI 3121.01B *supra* note 18, encl. A, para.2.c.
[159] CJCSI 3121.01B *supra* note 18, encl. A, para.2.c.
[160] CJCSI 3121.01B *supra* note 18, encl. A, para.2.b.
[161] *See* CJCSI 3121.01B *supra* note 18, encl. L.

approval.[162] Differences in the SRUF largely arise from the fact that the SRUF incorporate protections to civilians granted in U.S. law, especially the U.S. Constitution.[163] In circumstances where the SRUF apply outside the United States, providing those protections acknowledges that those operations are in a permissive environment and the military is supporting a functioning local government rather than replacing it.[164] In those cases, DoD personnel need force protection because of their presence and not because they are there to engage in hostilities.[165] Some may argue that applying the RUF in FDR missions is overly protective, since foreign citizens do not hold rights under the U.S. Constitution in their own countries. However, the DoD already uses RUF in overseas missions, like protection of U.S. installations and some force protection missions.[166]

There is no option under the SRUF to declare a force "hostile."[167] The SRUF balance commanders' force protection requirements with respect for human rights. The first procedure listed under the SRUF is de-escalation, stating that "when time and circumstance permit, the threatening force should be warned and given the opportunity to withdraw or cease threatening actions."[168] It goes on to emphasize that force of any kind will be "used only as a last resort, and the force used should be the minimum necessary."[169] Deadly force is authorized "when all lesser means have failed or cannot reasonably be employed" and only under specified circumstances when lives are in danger.[170] Otherwise, only limited uses of deadly force are authorized, and only when in direct support of the mission.[171]

The SRUF emphasize restraint and narrow the times when Service members can use force. Conversely, the goal in formulating ROE is "to ensure they allow maximum flexibility for mission accomplishment while providing clear, unambiguous guidance to the forces affected."[172] The SRUF only authorize deadly force in situations where lives are at stake,

---

[162] CJCSI 3121.01B *supra* note 18, encl. L, para. 3.a.
[163] Major Daniel Sennott, *Interpreting Recent Changes to the Standing Rules for the Use of Force*, ARMY LAW., Nov. 2007, at 52, 53, 58.
[164] *See* ROE V. RUF, *supra* note 37, at 2.
[165] ROE V. RUF, *supra* note 37, at 2.
[166] *See* CHAIRMAN, JOINT CHIEFS OF STAFF, INSTR. 3121.01B, STANDING RULES OF ENGAGEMENT/STANDING RULES FOR THE USE OF FORCE FOR U.S. FORCES, encl. L, para. 1.a (13 June 2005).
[167] *See id.* encl. L (providing no opportunity throughout the entirety of the Standing Rules of Engagement to declare a force "hostile").
[168] *Id.* encl. L, para. 5.a.
[169] *Id.* encl. L, para. 5.b.(1).
[170] *Id.* encl. L, para. 5.c.
[171] *Id.* encl. L, para. 5.d.
[172] *Id.* encl. I, para. 2a.

and not where necessary solely for mission accomplishment.[173] Furthermore, the SRUF anticipate that it may not be the only binding authority on the use of force; they specifically state that "host nation laws and international agreements may limit U.S. forces means of accomplishing their law enforcement or security duties."[174]

Commanders know they must prepare for the operating environment to change rapidly. Should the environment cease to be permissive—because the local government becomes unwilling or unable to provide force protection in the area where forces are operating—a commander should rightfully ask if RUF are sufficient. If the situation on the ground changes so much that RUF are insufficient, then the entire mission is changing. Potentially, it may mean withdrawal, or it may mean moving to an offensive posture where new ROE are appropriate. Even if forces were operating under more RUF-like ROE, like those used in Haiti, retraining and reorienting would be necessary when the mission changes.

Foreign disaster relief is one tool that the United States can employ to stabilize and support allied governments and create international goodwill when disaster strikes. Therefore, the United States should take action that will foreseeably improve its chances of mission success. The next section discusses how using the SRUF instead of the SROE will help leaders put their Soldiers, Airmen, Sailors, and Marines in the best possible position to succeed.

B. Helping Service Members Achieve Mission Success

Using RUF instead of ROE will better prepare Service members to conduct FDR missions, decrease the chances of conflict, better protect them while they are operating in foreign jurisdictions, and help JAs accurately and swiftly advise commanders planning FDR missions. Using RUF changes the way the command trains Service members. Going back to the doctrinal definition of ROE, they control how Service members "initiate and/or continue combat engagement with other forces encountered."[175] This emphasis on combat translates to an emphasis on

---

[173] *Id.* encl. L, para. 5.d.(1); See *infra* Appendix A for the full text of Standing Rules for the Use of Force.

[174] *Id.* encl. L, para. 1a.

[175] JOINT CHIEFS OF STAFF, JOINT PUB. 1-02, DICTIONARY OF MILITARY AND ASSOCIATED TERMS 207 (8 Nov. 2010) (C1 15 Feb. 2016).

combat vignettes when training on ROE.[176] Individuals trained in "combat engagement" are generally training to expect the declaration of a hostile force.[177] In humanitarian situations, training de-escalation and strictly limiting uses of force may be better choices to accomplish the mission.[178]

On 20 May 1997, a Marine corporal assigned to patrol the Texas border on an anti-drug mission shot and killed a U.S. citizen.[179] At the time, he was operating under ROE.[180] When the Marine perceived a civilian had a weapon and was firing it in his team's direction believing his team was under threat, he returned fire and killed the civilian.[181] The State of Texas, the U.S. Department of Justice, and the military all conducted investigations of the incident, but there were no indictments.[182] There was no evidence that the Marines were, in fact, under threat from the civilian.[183] At the time, no SRUF existed.[184] Some scholars felt that the Marine would have perceived the threat differently and acted differently if he had received training better tailored to a domestic mission.[185] Others felt that the fact that there was no indictment is evidence that the DoD does not need specialized rules to protect Service members, because self-

---

[176] This assertion is based on the author's recent professional experiences developing and delivering ROE briefs as Group Judge Advocate, 4th Psychological Operations Group (Airborne), Ft. Liberty, North Carolina, 2020–2021; Command Judge Advocate, 16th Military Police Brigade, Ft. Liberty, North Carolina, 2018–2020; Operational Law Attorney, United States Army Africa/Southern European Task Force, Vicenza, Italy, 2017–2018; Operational and Administrative Law Attorney, and 173d Infantry Brigade Combat Team (Airborne), Vicenza, Italy. *E.g.* CTR. FOR ARMY LESSONS LEARNED, HANDBOOK NO. 11-26, ROE VIGNETTES OBSERVATIONS, INSIGHTS, AND LESSONS (May 2011) [hereinafter Professional Experience].

[177] *See* ROE V. RUF, *supra* note 37; Professional Experience, *supra* note 176.

[178] *See* ROE V. RUF, *supra* note 37.

[179] ROE V. RUF, *supra* note 37, at 1.

[180] Jesse Katz, *Marines Faulted in Own Report on Teen's Death*, L.A. TIMES (Sept. 20, 1998), https://www.latimes.com/archives/la-xpm-1998-sep-20-mn-24833-story.html.

[181] *Id.*

[182] *See* ROE V. RUF, *supra* note 37, at 1; Katz, *supra* note 180.

[183] *See* ROE V. RUF, *supra* note 37, at 1; Katz, *supra* note 180.

[184] ROE V. RUF, *supra* note 37, at 2–3. The various documents controlling RUF were consolidated into CJCSI 3121.01B after September 11, when the DoD became involved in homeland defense efforts. The SRUF in their current state were developed in 2005 with the publication of the current CJCSI 3121.01B. *See* CJCSI 3121.01B *supra* note 18, at 1.

[185] *See* ROE V. RUF, *supra* note 37; W. Hays Parks, *Deadly Force Is Authorized*, 127 U.S. NAVAL INST. PROC. 1 (2001). The thesis of the Parks article is that overly restrictive ROE handicap and endanger U.S. forces, which seems to run contrary to the thesis of this paper. *See* Parks, *supra* at 1. However, the situation described by Parks is one where leaders neither understand nor teach self-defense well, and the rules applicable at the time predate the current standing rules. *See* Parks, *supra* at 1.

defense is already a legal defense.[186] However, the issue is about more than whether or not criminal liability will attach. This event, and the fallout in the media, effectively ended the DoD mission at the border in that form; in fact, the DoD did not use regular military forces to patrol the southwest border in support of the U.S. Border Patrol again until the "Faithful Patriot" deployment in 2018.[187]

A 1992 incident demonstrates how Service members that do not receive specific training can inadvertently fall back on general training in ways that can potentially be disastrous for the mission. This incident gave proof to the quotation popularly ascribed to the Greek poet Archilochus, "We do not rise to the level of our expectations, we fall to the level of our training."[188] Marines detailed to assist local law enforcement during the Los Angeles riots provided support to police at a private home where a domestic disturbance was underway.[189] When the local police knocked, birdshot fired from inside the house struck the police officers.[190] The officers shouted "cover me" to the Marines, by which the police officers meant get your weapons ready and keep your eyes open.[191] To the Marines however, that phrase meant lay down fire.[192] The Marines fired an estimated 200 rounds into the house, though amazingly no one was hurt.[193] Had someone been hurt, one can only imagine the fallout in the media and public perception of the DoD mission in Los Angeles.

Service members trained in ROE have that mentality locked in their minds. Using ROE for FDR that looks identical to the ROE used on a deployment, with slight modifications, may not be sufficient to switch from a battlefield mindset to a humanitarian mission mindset. Foreign

---

[186] Lieutenant Colonel Mark Martins, *Deadly Force is Authorized, but Also Trained*, ARMY LAW., Sept./Oct. 2001, at 1, 6.

[187] Manny Fernandez, *U.S. Troops Went to the Border in 1997. They Killed an American Boy,* N.Y. TIMES (Nov. 27, 2018), https://www.nytimes.com/2018/11/27/us/esequiel-hernandez-death-border-mexico.html; David Ignatius, *Mattis is Walking the Trump Tightrope. It's Agonizing to Watch,* WASH. POST, (Nov. 1, 2018), https://www.washingtonpost.com/opinions/mattis-is-walking-the-trump-tightrope-its-agonizing-to-watch/2018/11/01/9f712962-de0e-11e8-b732-3c72cbf131f2_story.html. Use of the operation name "Faithful Patriot" ended shortly before the midterm elections in 2018 because some felt it had "political overtones." Nancy Youssef, *Pentagon Dropping Use of 'Faithful Patriot' as Name for Border Deployment*, WALL ST. J., (Nov. 7, 2018), https://www.wsj.com/articles/pentagon-dropping-use-of-faithful-patriot-as-name-for-border-deployment-1541605581.

[188] JOHN F. ANTAL, LEADERSHIP RISING 78 (2021); Sennott, *supra* note 163, at 67.

[189] Sennott, *supra* note 163, at 66–67.

[190] Sennott, *supra* note 163, at 66.

[191] Sennott, *supra* note 163, at 66-67.

[192] Sennott, *supra* note 163, at 67.

[193] Sennott, *supra* note 163, at 67.

disaster relief missions are distinguishable from combat missions, and the definition of success is different. The use of force training needs to be distinguishable also, or the DoD is jeopardizing its own success.

Leaders should also be concerned about protecting Service members' due process rights when they are performing duties in a foreign jurisdiction.[194] If a SOFA is in place granting exclusive jurisdiction to the United States, then uses of force by Service members will be subject to U.S. jurisdiction and protections. If there is no SOFA, uses of force may be subject to local law.[195] Even with a SOFA, frequently the United States is not granted exclusive jurisdiction, meaning that the United States may need to prove additional facts before it can claim jurisdiction. For example that the action in question was taken as a part of official duties, or that the victim was a U.S. citizen. [196] This is especially challenging in FDR missions because the DoS does not know what country will need assistance and cannot predict if a favorable agreement will be in place.

If the host nation may have jurisdiction, several issues could put Service members at further legal risk. For example, the United States allows for "anticipatory self-defense," a concept in U.S. security law that other nations frequently do not recognize.[197] Additionally, "legal duty" and "obedience to orders" may be an excuse in some cases under the Uniform Code of Military Justice, but not local law.[198] By using ROE instead of RUF, the DoD encourages Service members to take more risk in the course of their duties. United States commanders will not be able to protect Service members' due process in areas with insufficient SOFA protections. Appendix B contains a table showing the top ten countries most affected by climate change in the last twenty years and lists their SOFA status for an idea of the risks should the DoD provide FDR in these countries in the future. Because of their vulnerability to climate change, these countries are at higher risk of a disaster requiring USG assistance. If the DoD deploys to these countries, Service members will not have the benefit of an established SOFA in at least half of them, and only partial jurisdiction in three more. In many countries where Service members may deploy to provide FDR, they are at risk of being subject to the local law and jurisdiction.

---

[194] INT'L SEC. ADVISORY BD., REPORT ON STATUS OF FORCES AGREEMENTS 11–14 (2015).
[195] *Id.*
[196] Lieutenant Colonel W. A. Stafford, *How to Keep Military Personnel from Going to Jail for Doing the Right Thing: Jurisdiction ROE and the Rules of Deadly Force*, ARMY LAW., Nov. 2000, at 1, 8.
[197] *Id.* at 20.
[198] *Id.*

Finally, the development of appropriate RUF is less time-consuming and RUF training is easier to deliver clearly, providing a direct benefit to Service members. Training RUF is one of the Judge Advocate General's Corps's enumerated collective tasks, so a JA in a national security law position should be able to brief it.[199] Support to massive disasters is difficult to plan. Frequently in rapid deployment situations, commanders are not contemplating the use of force until the deployment order arrives.[200] Judge advocates may have to scramble to squeeze ROE into a humanitarian context.[201] Starting with the SROE forces JAs and commanders to contrive ROE from scratch that meet U.S. goals and requirements, and the requirements of the host nation and international law. It also forces them to anticipate every scenario where authority to use force should be held to a higher level. If the team developing the guidelines for the use of force start with the SRUF, it already addresses many of these considerations. And as the SRUF is restrictive, the team does not have to foresee every possible use of force that a subordinate commander may authorize.[202]

The next section will discuss how uses of force, even if they are justified or just contemplated, can derail an FDR mission if it fails to communicate the mission's true goals. When leaders fail to ensure their Service members are well-trained and prepared for the mission at hand, they increase the chance a small incident escalating and changing the international perception of military actions.

C. Public Affairs and International Perceptions

As the media gains access to military operations and look for a worldwide audience, incidents that result in civilian casualties are held to increasing levels of scrutiny by both the American public and international

---

[199] U.S. DEP'T OF ARMY, FIELD MANUAL 1-04, LEGAL SUPPORT TO OPERATIONS app. C, tbl.C-1 (8 June 2020) (stating that training RUF is a collective task in support of the warfighting functions movement and maneuver and command and control).

[200] This assertion is based on the author's recent professional experiences preparing for multiple rapid domestic deployments and operations as Command Judge Advocate, 16th Military Police Brigade, Ft. Liberty, North Carolina, 2018–2020.

[201] *See* JP 3-29 *supra* note 14.

[202] *See supra* Part IV for difficulties of reworking ROE in Honduras and ROE development in Haiti in the midst of a complex rapid deployment of forces.

audiences.[203] This increased level of scrutiny may lead to less public and political support from American and international communities.[204] If a part of the U.S. purpose in conducting FDR is demonstrating good-will and earning the trust and respect of international partners, bad press can mean mission failure. If the mission loses political support, it may lose funding before it meets its objectives, and again the mission will fail. Civilian casualties can rarely be pinned on one thing that went wrong at one level of command, but ambiguity in the guidelines governing the use of force will be one contributing factor.[205]

The DoD public affairs office can also take a lesson from Haiti, and should encourage transparency.[206] Unlike the SROE, the SRUF is unclassified, and thus a public affairs officer can share it with partner forces and the media freely.[207] Transparency may go a long way to assuring the media and international partners about the true goal and purpose of the use of force. If the public affairs officer can release the SRUF and show how an action fell under it, it may allow the United States to continue to demonstrate its good will.

The DoD cannot control the narrative of FDR missions, but it can decide to influence the message or passively let the narrative control the mission. The case study on Haiti lays out a scenario where the media and global perceptions threatened to become more persuasive to the global community than the DoD public affairs plan. United States competitors are only too eager to seize a slip-up to spin U.S. humanitarian action in a way that favors their own interests, whether that be to portray the United States as conducting an offensive attack, colonizing, or just being generally careless about the lives and livelihoods of citizens of developing nations. The public affairs officer's role to distribute information about the U.S. mission to U.S. and international audiences and to stay linked to the media is especially important during delicate operations like FDR.[208]

Looking forward, leaders in the legal field foresee changes to the legal environment in which the United States fights it wars. The next section will explore how these changes may affect the SROE and argue that it will become even less applicable to the goals of FDR.

---

[203] Major Sherry K. Oehler, The Unintended Consequences of Killing Civilians 8 (2012) (Monograph, School of Advanced Military Studies, United States Army Command and General Staff College) (on file with the Defense Technical Information Center).
[204] *Id.*
[205] *Id.* at 50.
[206] *See supra* Part IV.B.
[207] JOINT CHIEFS OF STAFF, JOINT PUB. 3-61, PUBLIC AFFAIRS, app. C para. 2.c.(4) (14 May 2019).
[208] *See* JP 3-29, *supra* note 14, at IV-3.

D. Transition to Large-Scale Combat Operations

In 2017, the U.S. Army started to refocus its attention on LSCO.[209] Army leaders recognized that while the Army focused on counterterrorism and counterinsurgency, U.S. near-peer competitors were developing their own military power.[210] During that time, the Army developed gaps in its conventional warfighting capabilities, putting the United States at risk in a LSCO situation.[211] As the Army shifts its focus to man, train, and equip for LSCO, JA leaders are reevaluating how they recommend leaders draft and apply ROE.[212]

Lieutenant General Charles Pede, formerly The Judge Advocate General of the U.S. Army, identified gaps in the DoD's legal preparation and training as well.[213] He describes the ROE developed for counterinsurgency operations as "constrained" when compared to the broader authorities permitted under the law of armed conflict.[214] Rules of engagement are policy, and that policy has been conservative, withholding strikes based on status to high levels.[215] Policymakers may take LTG Pede's recommendation and redesign the SROE to adhere to the law of war more closely and move it further from a policy-based structure that "serve[s] humanitarian purposes."[216] If that happens, the SROE will become even harder to apply to FDR missions.

VI. Conclusion

The timing is right to reevaluate the rules of engagement and rules for the use of force and their application to military missions. The national security law world has expected a revision to the SRUF and SROE for

---

[209] *See* U.S. DEP'T OF ARMY, FIELD MANUAL 3-0, OPERATIONS (6 Oct. 2017).
[210] Lieutenant General Michael D. Lundy, *Meeting the Challenge of Large-Scale Combat Operations Today and Tomorrow*, MIL. REV., Sept.-Oct. 2018, at 111, 112.
[211] Lieutenant General Charles Pede & Colonel Peter Hayden, *The Eighteenth Gap: Preserving the Commander's Legal Maneuver Space on "Battlefield Next,"* MIL. REV., Mar.-Apr. 2021, at 6.
[212] *Id.* at 7.
[213] *See id.* at 6-7.
[214] *Id.* at 7.
[215] *See id.* at 7.
[216] *Id.* at 10.

years.[217] The joint chiefs published the current version in 2005, and it is ripe for revision based on the changes in the operational and training goals of the DoD.[218] Some may say that there is no need to change, because FDR missions have used ROE without catastrophic issues for years. However, the case studies above demonstrate that deployed leaders and JAs on these missions who worked hard to make the ROE more like a RUF deserve credit for their success. They built rules that emphasize de-escalation over engagement and comply with the U.N. goal of humanity, neutrality, and impartiality.

Returning to the opening hypothetical, one should consider how implementing the SRUF would have changed the outcome. When the machete-wielding man surprised the scout team, robust RUF training would have provided tools to deescalate the situation. When the commander sensed danger and feared an ambush, his RUF training would have urged him to safely withdraw rather than to send scouts. And if the brigade intelligence element detected possible hostile actors in the region, the command would never have sent engineers to that project on that day.

In sum, applying the SRUF to FDR missions makes more sense. It will allow leaders to focus troops on the mission at hand and separate the battlefield mindset from the humanitarian mission mindset. It has value in how it will change the public perception of DoD action in FDR missions, allowing the United States to say that the DoD is treating the victims of the natural disaster as if they were U.S. citizens. It allows the military to better comply with international norms and expectations and with U.S. rules and foreign policy goals. It will ease the burden on JAs scrambling to train and deploy with their unit. Finally, it anticipates changes to our operational environment caused by climate change. It also anticipates a pivot to LSCO operations to ensure that FDR remains focused on relieving human suffering and saving lives.

---

[217] *See* NAT'L SEC. L. DEP'T, THE JUDGE ADVOC. GEN.'S LEGAL CTR. & SCH., U.S. ARMY, OPERATIONAL LAW HANDBOOK 105 (2021) (stating "The 2005 version remains the most current publication of the SROE"); NAT'L SEC. L. DEP'T, THE JUDGE ADVOC. GEN.'S LEGAL CTR. & SCH., U.S. ARMY, OPERATIONAL LAW HANDBOOK 6 (2016) (stating "A new version of the CJCSI is due for publication in 2014. At the time of this publishing the new SROE was not available."); NAT'L SEC. L. DEP'T, THE JUDGE ADVOC. GEN.'S LEGAL CTR. & SCH., U.S. ARMY, OPERATIONAL LAW HANDBOOK 75 (2012) (stating CJCSI 3121.01B was "under revision").

[218] As briefly discussed in section V.D., as the Army is shifting to large-scale combat operations, it may impact the SROE. Developments in multi-domain warfare may also prompt change.

Appendix A

UNCLASSIFIED

CJCSI 3121.01B
13 June 2005

ENCLOSURE L

STANDING RULES FOR THE USE OF FORCE FOR US FORCES

1. Purpose and Scope

a. Standing Rules for the Use of Force (SRUF) provide operational guidance and establish fundamental policies and procedures governing the actions taken by DOD forces performing civil support missions (e.g., military assistance to civil authorities and military support for civilian law enforcement agencies) and routine Service functions (including AT/FP duties) within US territory (including US territorial waters). The SRUF also apply to land homeland defense missions occurring within US territory and to DOD forces, civilians and contractors performing law enforcement and security duties at all DOD installations (and off-installation, while conducting official DOD security functions), within or outside US Territory, unless otherwise directed by the SecDef. Host nation laws and international agreements may limit US forces means of accomplishing their law enforcement or security duties. Additional examples of these missions, within the US, include protection of critical US infrastructure both on and off DOD installations, military assistance and support to civil authorities, DOD support during civil disturbance and DOD cooperation with Federal, State and local law enforcement authorities, including counterdrug support.

b. SRUF cancels CJCSI 3121.02, "RUF for DOD Personnel Providing Support to Law Enforcement Agencies Conducting CD Operations in the United States," and RUF contained in DOD Civil Disturbance Plan (Garden Plot). Existing standing Military Department and combatant commander RUF directives shall be reviewed and updated to comply with these SRUF. Existing SecDef-approved mission-specific RUF remain in effect, unless otherwise noted. Use of force guidance contained in this instruction supercedes that contained in DOD Directive 5210.56, Enclosure 2.

c. Unit commanders at all levels must teach and train their personnel how and when to use both non-deadly and deadly force in self-defense.

d. DOD forces detailed to other USG lead Federal Agencies (LFA) (e.g., support to US Border Patrol) will operate under common mission-

UNCLASSIFIED

specific RUF approved by the SecDef and the LFA. DOD forces always retain the right of self-defense, IAW these SRUF.

e. DOD forces under USCG control, conducting operations both outside and within the territorial limits of the US, will follow the Use of Force Policy for warning shots and disabling fire as issued by the Commandant, USCG, per 14 USC 637 (reference w). DOD forces, under USCG control and inside the territorial limits of the US, retain the right of self-defense IAW these SRUF.

f. DOD forces, under DOD control (and using DOD SRUF and mission-specific RUF), but operating in coordination with other LFA security forces, will coordinate with on-scene LFA personnel to ensure common understanding of DOD RUF. Combatant commanders shall notify the SecDef, through the CJCS, of any use of force issues that cannot be resolved.

2. Policy. Unit commanders always retain the inherent right and obligation to exercise unit self-defense in response to a hostile act or demonstrated hostile intent. Unit self-defense includes the defense of other DOD forces in the vicinity.

3. Combatant Commander Mission-Specific RUF

a. Combatant commanders may augment these SRUF as necessary by submitting a request for mission-specific RUF to the CJCS for SecDef approval. The message format for requesting approval of mission-specific RUF is contained in Enclosure P.

b. Unit commanders may further restrict mission-specific RUF approved by the SecDef. US commanders shall notify the SecDef, through the CJCS, as soon as practicable, of restrictions (at all levels) placed on Secretary of Defense-approved RUF. In time critical situations, make SecDef notification concurrently to the CJCS. When concurrent notification is not possible, notify the CJCS as soon as practicable after SecDef notification.

c. Combatant commanders will distribute these SRUF to subordinate commanders and units for implementation.

4. Definitions and Authorities

a. Inherent Right of Self-Defense. Unit commanders always retain the inherent right and obligation to exercise unit self-defense in response to a hostile act or demonstrated hostile intent. Unless otherwise directed by a unit commander as detailed below, service members may exercise individual self-defense in response to a hostile act or demonstrated hostile intent. When individuals are assigned and acting as part of a unit, individual self-defense should be considered a subset of unit self-defense. As such, unit commanders may limit individual self-defense by members of their unit.

b. Imminent Threat. The determination of whether the danger of death or serious bodily harm is imminent will be based on an assessment of all facts and circumstances known to DOD forces at the time and may be made at any level. Imminent does not necessarily mean immediate or instantaneous. Individuals with the capability to inflict death or serious bodily harm and who demonstrate intent to do so may be considered an imminent threat.

c. Hostile Act. An attack or other use of force against the United States, US forces or other designated persons or property. It also includes force used directly to preclude or impede the mission and/or duties of US forces, including the recovery of US personnel or vital USG property.

d. Hostile Intent. The imminent threat of the use of force against the United States, US forces or other designated persons or property. It also includes the threat of force to preclude or impede the mission and/or duties of US forces, including the recovery of US personnel or vital USG property.

e. Assets Vital to National Security. For the purposes of DOD operations, defined as President-designated non-DOD and/or DOD property, the actual theft or sabotage of which the President determines would seriously jeopardize the fulfillment of a national defense mission and would create an imminent threat of death or serious bodily harm. Examples may include, but are not limited to, nuclear weapons; nuclear command and control facilities; and designated restricted areas containing strategic operational assets, sensitive codes or special access programs.

f. Inherently Dangerous Property. Property is considered inherently dangerous if, in the hands of an unauthorized individual, it would create an imminent threat of death or serious bodily harm. Examples may include, but are not limited to: portable missiles, rockets, arms, ammunition, explosives, chemical agents and special nuclear materials. On-scene DOD commanders are authorized to classify property as inherently dangerous.

g. National Critical Infrastructure. For the purposes of DOD operations, defined as President-designated public utilities, or similar critical infrastructure, vital to public health or safety, the damage to which the President determines would create an imminent threat of death or serious bodily harm.

5. Procedures

a. De-Escalation. When time and circumstances permit, the threatening force should be warned and given the opportunity to withdraw or cease threatening actions.

b. Use of Non-Deadly Force

(1) Normally, force is to be used only as a last resort, and the force used should be the minimum necessary. The use of force must be reasonable in intensity, duration and magnitude based on the totality of circumstances to counter the threat. If force is required, non-deadly force is authorized and may be used to control a situation and accomplish the mission, or to provide self-defense of DOD forces, defense of non-DoD persons in the vicinity if directly related to the assigned mission, or in defense of the protected property, when doing so is reasonable under the circumstances.

(2) The use of Service-approved, unit issued non-lethal weapons and riot control agents, including oleoresin capsicum (OC) pepper spray, and CS gas, is authorized in operations other than war. Detailed guidance for use of riot control agents by DOD personnel is governed by CJCSI 3110.07 Series, (references b and t listed in Enclosure K).

(3) When operating under SRUF, warning shots are not authorized within US territory (including US territorial waters), except when in the appropriate exercise of force protection of US Navy and Naval Service vessels within the limits set forth in Enclosure M.

Appendix B

	Long-Term Climate Risk Index Countries[219]	SOFA Condition[220]
1	Puerto Rico	N/A[221]
2	Myanmar/Burma	none
3	Haiti	A&T protections[222]
4	Philippines	Less than exclusive jurisdiction[223]
5	Mozambique	A&T protections[224]
6	The Bahamas	unknown[225]
7	Bangladesh	none
8	Pakistan	none
9	Thailand	none
10	Nepal	none

[219] The Long-Term Climate Risk Index ranks the top ten countries most affected from 2000 to 2019 by their annual averages. GCRI 2021 *supra* note 1, at 13.

[220] For a list of all U.S. treaties in force as of 2020, see U.S. DEP'T OF STATE, TREATIES IN FORCE: A LIST OF TREATIES AND OTHER INTERNATIONAL AGREEMENTS OF THE UNITED STATES IN FORCE ON JANUARY 1, 2020 (2020) [hereinafter 2020 TREATIES IN FORCE].

[221] Puerto Rico is an unincorporated territory of the United States; a status of forces agreement is not applicable.

[222] Agreement Regarding the Status of U.S. Military Personnel and Civilian Employees of the Department of Defense Temporarily in Haiti in Connection with their Official Duties., Haiti-U.S., May 10–11, 1995, T.I.A.S. No. 95-511. United States military personnel enjoy the same status as that provided to the administrative and technical staff of the U.S. Embassy.

[223] Agreement Regarding the Treatment of United States Armed Forces Visiting the Philippines, Phil.-U.S., Feb. 10, 1998, T.I.A.S. No. 12931.

[224] Agreement Concerning the Status of United States Military and Civilian Personnel of the U.S. Department of Defense Temporarily Present in Mozambique in Connection with Humanitarian Relief Operations, Mozam.-U.S., Mar. 3–7, 2000, T.I.A.S. No. 00-307.1.

[225] Agreement Regarding U.S. Military and Civilian Personnel and U.S. Contractors Who May be Temporarily Present in the Bahamas in Connection with Humanitarian Assistance and Disaster Relief and Recovery Efforts, Bah.-U.S., Sept. 11, 2019, 2020 TREATIES IN FORCE, *supra* note 220, at 24.

THIS PAGE INTENTIONALLY LEFT BLANK

EXPLOITATION

LIEUTENANT COLONEL GREGG CURLEY*

I. Introduction

Service members reported 6,290 military sexual assaults (MSAs) in 2020, up from 6,236 in 2019.[1] This number may represent as little as 30 percent of the actual number of MSAs that occurred during that fiscal year.[2] Military sexual assaults erode combat readiness, public trust of the military, lethality, and unit cohesion.[3] The physical and emotional impacts that MSA victims suffer can, and often do, last a lifetime. In 2015 alone, the U.S. Veterans Administration reported 1.3 million outpatient visits for care related to military sexual trauma.[4] As a matter of perception,

---

* Judge Advocate, U.S. Marine Corps. Presently assigned as the Commanding Officer, 3d Recruit Training Battalion, Marine Corps Recruit Depot Parris Island; MMS, 2019, Marine Corps Command and Staff College; MMOAS, 2017, Air Command and Staff College; LL.M., 2015, The Judge Advocate General's Legal Center and School, U.S. Army; J.D., 2008, Roger Williams University School of Law; MBA, 2005, and BS, 2004, Sacred Heart University. Previous assignments include Officer in Charge of the Legal Services Support Team, Senior Trial Counsel, Complex Trial Counsel, Defense Attorney, Civil Affairs Team Leader (Fwd.), Aide-de-Camp, and Special Assistant United States Attorney. Member of the Bar of Massachusetts and admitted to practice before the Court of Appeals for Veterans Claims, Court of Appeals for the Armed Forces, and the Supreme Court of the United States. A version of this paper was submitted in partial completion of Senior Developmental Education, Air War College Distance Program.

[1] Press Release, U.S. Dep't of Def., Department of Defense Releases Fiscal Year 2020 Annual Report on Sexual Assault in the Military (May 13, 2021), *U.S. Department of Defense*, May 13, 2021, https://www.defense.gov/News/Releases/Release/Article/2606508/department-of-defense-releases-fiscal-year-2020-annual-report-on-sexual-assault/mslkid/department-of-defense-releases-fiscal-year-2020-annual-report-on-sexual-assault; Howard Altman, *In One of First Actions, New Defense Secretary Orders Review of Sexual Misconduct Programs*, MIL. TIMES (Jan. 23, 2021), https://www.militarytimes.com/news/your-military/2021/01/24/in-one-of-first-actions-new-secdef-orders-review-of-sexual-misconduct-programs (citing Department of Defense Fiscal Year 2019 Annual Report on Sexual Assault in the Military).

[2] Altman, *supra* note 1.

[3] *See generally* INDEP. REV. COMM'N ON SEXUAL ASSAULT IN THE MIL., HARD TRUTHS AND THE DUTY TO CHANGE: RECOMMENDATIONS FROM THE INDEPENDENT REVIEW COMMISSION ON SEXUAL ASSAULT IN THE MILITARY (2021) [hereinafter, IRC REPORT].

[4] Altman, *supra* note 1.

commentators and decision makers have described MSA as "an epidemic,"[5] "a plague,"[6] and "a scourge."[7] Civilian leaders of the Department of Defense (DoD), members of Congress, and the current presidential administration are unequivocal: the amount of sexual misconduct in the military is unacceptable.

The impetus for reform is more pronounced than ever. Within the first forty-eight hours following his confirmation, Secretary of Defense (SecDef) Lloyd Austin tasked senior leadership with assessing which Sexual Assault Prevention and Response (SAPR) programs work, which do not, and to share any novel solutions to the problem.[8] The President echoed SecDef's call for action, ordering a comprehensive ninety-day review of MSA that began on 24 March 2021.[9] The Independent Review Commission (IRC) completed this review in June of 2021.[10] The DoD will fully implement the IRC's eighty-two recommendations.[11]

The prologue to the present has not been promising. While the inability to satisfactorily address MSA has many root causes, inaction is not one of them. More than ten DoD Inspector General engagements have occurred since 2010 to review and improve SAPR.[12] The Secretary of Defense directed more than fifty initiatives to improve prevention and response; the DoD operationalized more than 150 congressional MSA-related provisions;[13] the individual military departments evaluated more than 200 "recommendations from government panels and task forces . . . for applicability to the SAPR mission [set]";[14] and the Government

---

[5] *Mission: Ending the Epidemic of Military Rape*, PROTECT OUR DEFENDERS, https://www.protectourdefenders.com/about (last visited Apr. 10, 2023).

[6] Altman, *supra* note 1.

[7] Col William Bowers, How to Eradicate a Scourge (2019) (U.S. Marine Corps University), https://www.usmcu.edu/Portals/218/LLI/CCSPW/Bowers%20Col%20WJ%20-%20How%20To%20Eradicate%20a%20Scourge.pdf?ver=2019-04-26-162157-347.

[8] Memorandum from Sec'y of Def. to Sr. Pentagon Leadership et al., subject: Countering Sexual Assault and Harassment – Initial Tasking (23 Jan. 2021) [hereinafter, SecDef Memo].

[9] *See* IRC REPORT, *supra* note 3, at 3.

[10] *Id.*

[11] Memorandum from Sec'y of Def. to Sr. Pentagon Leadership et al., subject: Commencing DoD Actions and Implementation to Address Sexual Assault and Sexual Harassment in the Military (22 Sept. 2021); *see also* C. Todd Lopez, "DOD Takes Phased Approach to Implementing Recommendations on Sexual Assault, Harassment," DOD NEWS (July 21, 2021), https://www.defense.gov/Explore/News/Article/Article/2702095/dod-takes-phased-approach-to-implementing-recommendations-on-sexual-assault-har.

[12] IRC REPORT, *supra* note 3, at 12.

[13] IRC REPORT, *supra* note 3, at 12.

[14] IRC REPORT, *supra* note 3, at 12. The Department of the Navy refers to this field as Sexual Assault Prevention and Response (SAPR); the Department of the Army refers to this field as Sexual Harassment/Assault Response and Prevention (SHARP).

Accountability Office has assessed more than sixty different initiatives "to measure prevention and response efforts and to inform future programming."[15] While mobilization on this issue has been significant, the return on investment is underwhelming. As Representative Jackie Speier noted after the publication of yet another assessment of MSA, "We've thrown about $200 million at this problem for eight to [ten] years, and this report suggests it's not working."[16]

Further complicating hopes for progress, military incidence rates roughly match those of comparable civilian populations. That similarity is hardly surprising: "seventy-three percent of military victims are ranks E-1 to E-4—in other words, junior-grade enlisted members whose ages, living situations, and behavior align with those of college students."[17] As law student, Andreas Kuersten, noted in Joint Forces Quarterly, "[T]he military's inability to fix the problem of sexual assault in its ranks is likely, at least in part, a reflection of the military's intimate connection to the broader community where the issue also remains pervasive."[18] Any expectations in this arena must be tempered by the understanding that this problem is not unique to the military.[19] No effort, discipline, approach, or resources can or will eradicate MSA. Even so, the military is held to a higher standard than its civilian counterpart and rightfully so. The DoD must do better.

In an effort to identify a meaningful reform, this paper will apply aspects of problem framing to the sexual assault problem set. Next, it proposes a presidentially-proscribed Article 134 crime: exploitation,[20] before explaining how codifying this new offense will provide more appropriate results for victims, create measured justice for perpetrators, and ensure effective means for facilitating good order and discipline. It will then conclude by proposing a method for implementing the recommended crime.

---

[15] IRC REPORT, *supra* note 3, at 12.
[16] Dave Philipps, *'This Is Unacceptable.' Military Reports a Surge of Sexual Assaults in the Ranks*, N.Y. TIMES (May 2, 2019), https://www.nytimes.com/2019/05/02/us/military-sexual-assault.html (quoting Congresswoman Jackie Speier).
[17] Andreas Kuersten, *Sexual Assault and the Military Petri Dish*, 74 JOINT FORCE Q., no. 3, 2014, at 91, 93.
[18] *Id.*
[19] *See id.*
[20] "Exploitation is the act of selfishly taking advantage of someone . . . in order to profit from them or otherwise benefit oneself." *Exploitation*, DICTIONARY.COM, https://www.dictionary.com/browse/exploitation (last visited Apr. 10, 2023).

II. Framing the Problem

If the first step to solving any problem is recognizing that a problem exists,[21] the next step is to properly understand the problem. As Marine Corps planning doctrine notes, "[N]o amount of subsequent planning can solve a problem insufficiently understood."[22] Past MSA reforms and current attempts at reform appear to be reactionary in nature, rather than the product of deliberate planning.

A. Scope

Military sexual assault is a *wicked problem,*[23] but the critical question is: "Why are [sexual] assaults happening in the first place?"[24] The answer to that question has little to do with military justice. Biology, social dynamics, environment, demographics, education, individual risk calculus, and prevention efforts all play roles more significant than military justice vis-à-vis the causal factors of MSA.[25] Thus, resource allocation and congressional attention should be proportionate. Military justice is not the panacea, yet it has been subject to a significant amount of congressional scrutiny and policy focus. The ability of criminal justice to reduce MSAs is limited; however, military justice can still exert some positive influence on the problem set. It provides the means to target the interrelated concepts of accountability and deterrence. Accountability begets deterrence; deterrence obviates accountability.

---

[21] In the opening scene of the first episode of HBO's series, *Newsroom*, Jeff Daniels' character, Will McAvoy, provides a famed speech to a crowd of students in which he states that "the first step in solving any problem is recognizing there is one." Attnjake, *HBO's NEWSROOM Opening Scene "Why America's Not the Greatest Country,"* YOUTUBE, at 4:11 (June 28, 2012), https://www.youtube.com/watch?v=zEyUWKJFER8.

[22] U.S. MARINE CORPS, MCWP 5-1, MARINE CORPS PLANNING PROCESS, at 1-5 (24 Aug. 2010) [hereinafter MCPP].

[23] *See* John C. Camillus, *Strategy as a Wicked Problem*, HARV. BUS. REV., May 2008, at 98; *What's a Wicked Problem?*, STONY BROOK U., https://www.stonybrook.edu/commcms/wicked-problem/about/What-is-a-wicked-problem (last visited Apr. 10, 2023) (explaining that the characteristics of wicked problems are innumerable causes, constant morphing, and lack of a clear answer).

[24] Melinda Wenner Moyer, '*A Poison in the System': the Epidemic of Military Sexual Assault*, N.Y. TIMES MAG. (Oct. 11, 2021), https://www.nytimes.com/2021/08/03/magazine/military-sexual-assault.html.

[25] *See Risk and Protective Factors,* CTRS. FOR DISEASE CONTROL AND PREVENTION, https://www.cdc.gov/violenceprevention/sexualviolence/riskprotectivefactors.html (last visited Apr. 10, 2023).

1. Accountability

The military justice system does not currently provide sufficient accountability for MSA. Constraints inherent in the system preclude a large proportion of MSA allegations from seeing a courtroom.[26] After a significant delay, those that do see a courtroom result in a significant number of acquittals.[27] The prevalence of acquittals, in the aggregate, is unacceptable. Without meaningful reform that addresses the constraints described below, the military justice system will continue to fail to provide adequate accountability or deterrence.

2. Deterrence

Accountability is vital to deterrence. General deterrence is derived from holding a Service member at personal criminal risk if they choose to break a law, regulation, policy, or violate a custom of the service.[28] The system does not currently hold potential offenders at sufficient risk to deter MSAs. Sentence certainty provides deterrent value; acquittals undermine that value.[29] As law professor Katharine Baker has explained, "[i]f behavior is not punished criminally because it cannot be proved, then the public's understanding of criminal behavior will not change."[30] The efficacy of any military justice reform should be assessed through the overall impact it will have on accountability and deterrence—the only two significant ways military justice contributes to MSA prevention.

---

[26] PROTECT OUR DEFENDERS, FACTS ON UNITED STATES MILITARY SEXUAL VIOLENCE (2018) ("In [Fiscal Year] 2017, of the 5,110 unrestricted reports of sexual assault and rape, only 406 (7.9%) cases were tried by court-martial and only 166 [41%] offenders were convicted of a nonconsensual sex offense.").

[27] *Id.* This assertion is also based on the author's experience from 2016-2021 as a senior trial counsel and complex trial counsel responsible for drafting and reviewing hundreds of case analysis memoranda as well as service as a defense counsel at the tactical and strategic levels from 2012-2016 [hereinafter Professional Experience].

[28] *See* Kelli D. Tomlinson, *An Examination of Deterrence Theory: Where Do We Stand?*, FED. PROBATION J., Dec. 2016, at 33, 33 (defining "general deterrence").

[29] U.S. DEP'T OF JUST., NAT'L INST. JUST., NATIONAL INSTITUTE OF JUSTICE: FIVE THINGS ABOUT DETERRENCE 1-2 (2016).

[30] Katharine K. Baker, *Why Rape Should Not (Always) Be a Crime*, 100 MINN. L. REV. 221, 223 (2015).

B. Background: Definitions of Sexual Misconduct and Its Treatment Within the Military

From 1775 until the Civil War, military commanders turned Service members accused of capital crimes, including rape, over to civilian prosecuting authorities.[31] Rape became subject to courts-martial in 1863—provided the crime was committed "in [a] time of war, insurrection, or rebellion."[32] The 1950 update to the Uniform Code of Military Justice (UCMJ) criminalized rape under the common law definition, requiring both the use of force and a lack of consent.[33] For the next thirty years, the crime of rape required corroboration, a fresh complaint, and, at trial, it permitted inquiry into the victim's sexual history.[34]

In 1980, the newly-created Military Rules of Evidence (MRE) eliminated the draconian requirements and established the "rape shield law," preventing inquiry into the victim's past sexual history in many circumstances.[35] From 1993 to 2006, there were no substantive changes to rape laws.[36] In 2006, Congress expanded Article 120 to include the criminal concept of sexual assault, focusing on lack of consent vice force or violence.[37] The statute received substantial clarifying revisions in 2011 and 2016.[38] Meanwhile, reforms to the MRE have continued, adding protections for victims and, in theory, making it easier for the Government to carry its burden.[39] The Article 120 procedural reforms are designed, in part, to make it more likely that an MSA case is tried before a court-

---

[31] *See* Jennifer Knies, *Two Steps Forward, One Step Back: Why the New UCMJ Rape Law Missed the Mark, and How an Affirmative Consent Statute Will Put it Back on Target,* ARMY LAW., Aug. 2007, at 1, 13 (citing American Articles of War (1776), reprinted in WILLIAM WINTHROP, MILITARY LAW & PRECEDENTS 964 (2d ed. 1920)).

[32] An Act of March 3, 1863, ch. 75, § 30, 12 Stat. 731, 736 (1863); s*ee also* Knies, *supra* note 31, at 13.

[33] Knies, *supra* note 31, at 13 (citing U.S. DEPT. OF ARMY, THE ARMY LAWYER: HISTORY OF THE JUDGE ADVOCATE GENERAL'S CORPS 1775-1975, at 203 (1976)).

[34] *See* Knies, *supra* note 31, at 13-15.

[35] Knies, *supra* note 31, at 13-14.

[36] Knies, *supra* note 31, at 14.

[37] *See* National Defense Authorization Act for Fiscal Year 2006, Pub. L. No. 109-163, §552, 119 Stat. 3136, 3256-63 (2006).

[38] 10 U.S.C. 920 (Amendments).

[39] *See* MANUAL FOR COURTS-MARTIAL, UNITED STATES, M.R.E. 404a, 412, 413, 513, 514 (2019) [hereinafter MCM].

martial,[40] but procedural reforms have failed to increase the likelihood of conviction in those forums.[41]

C. Constraints Inhibiting Accountability and Deterrence in Military Sexual Assault Cases

1. Sufficient Admissible Evidence

In many MSA cases, lack of accountability and deterrence stems from the prosecutor's inability to present sufficient evidence to meet the burden of proof at trial and then sustain the conviction on appeal. Commentators have recognized how hard it can be to prove nonconsensual sex between acquaintances.[42] In the author's experience, nearly every MSA case must contend with some or all the following hurdles: 1) no third-party eyewitnesses to the actual criminal conduct, 2) intoxication, 3) memory issues, 4) a pre-existing relationship, 5) motives to fabricate, and 6) delayed reporting.[43]

2. Lack of Eyewitnesses

Sexual assault is a private crime; usually the only two individuals present during an MSA are the victim and the accused. Whereas there are often many witnesses to the actions before and after a crime, rarely are there third-party witnesses that can provide a firsthand account of the MSA.[44] Interrogating a suspect is often of little utility, frequently resulting in an invocation or an assertion that the sexual act or contact was consensual.[45] The accused's constitutional right to remain silent can

---

[40] These reforms include special victims investigation and prosecution qualification requirements, National Defense Authorization Act for Fiscal Year 2013, Pub. L. No. 112-239, § 573, 126 Stat. 1653, 1755 (2013); changes to Article 32 hearings, UCMJ art. 32; sexual assault initial disposition authority requirements, U.S. MARINE CORPS, MCO P5800.15A, MARINE CORPS MANUAL FOR LEGAL ADMINISTRATION para. 1110 (31 Aug. 1999) (C7, 10 Feb. 2014).

[41] *See* PROTECT OUR DEFENDERS, FACTS ON UNITED STATES MILITARY SEXUAL VIOLENCE (2018).

[42] *See, e.g.*, Baker, *supra* note 30, at 223.

[43] *See* Baker, *supra* note 30, at 223.

[44] Baker, *supra* note 30, at 223.

[45] *See* SARAH MICHAL GREATHOUSE ET AL., A REVIEW OF THE LITERATURE ON SEXUAL ASSAULT PERPETRATOR CHARACTERISTICS AND BEHAVIORS 32 (2015).

completely preclude an accused's testimony, while memory issues and motives consistently undermine a victim's.[46]

3. Intoxication and Memory

In MSAs, the accused often utilizes alcohol as "a primary weapon."[47] In fact, in 61 percent of MSAs, alcohol is a factor.[48] Alcohol lowers the inhibitions of individuals under the influence and can cause memory issues.[49] Victims are often in a black-out state—walking, talking, and objectively functioning, but not encoding memories.[50] In these cases, defense attorneys can generate reasonable doubt by highlighting the gap in memory and/or filling that gap with plausible consensual explanations. With a victim's fragmented or non-existent memory and no eyewitnesses, the Government will generally be unable to reach the level of certainty required to obtain and sustain a conviction—in black-out cases, there is inherent reasonable doubt. While the effects of alcohol on a victim, without anything else, may often be sufficient to raise reasonable doubt, other common factors also work against the Government's ability to meet the burden of proof.

4. Pre-existing Relationships between the Victim and the Accused

The victim and the accused often have a pre-existing relationship—the majority of MSAs are committed by acquaintances.[51] Therefore, the frequently-present defense argument is that nearly every interaction between the accused and the victim tended to indicate consent, contributed

---

[46] *See infra* notes 47-61 and accompanying text.
[47] Bowers, *supra* note 7, at 5.
[48] Bowers, *supra* note 7, at 5; PSYCH. HEALTH CTR. OF EXCELLENCE, RAPID REVIEW OF ALCOHOL-RELATED SEXUAL ASSAULT/HARASSMENT IN THE MILITARY 1 (2020) (finding that "alcohol use by a victim or alleged offender was a factor in 62% of incidents involving [DoD] women").
[49] Aaron M. White, *What Happened? Alcohol, Memory Blackouts, and the Brain*, 27 ALCOHOL RSCH. & HEALTH 186, 186 (2003).
[50] *See* Hamin Lee, Sungwon Roh, and Dai Jin Kim, *Alcohol Induced Blackout,* 11 INT, J. ENVIRON. RES. PUBLIC HEALTH 2783, 2783 (2009).
[51] Patricia Kime, *Despite Efforts, Sexual Assaults Up Nearly 40% in US Military*, MIILTARY.COM (May 2, 2019), https://www.military.com/daily-news/2019/05/02/despite-efforts-sexual-assaults-nearly-40-us-military.html (stating that 62 percent of sexual assaults are perpetrated by an acquaintance).

to the accused's belief that the victim consented, or both.[52] While pre-existing relationships between the victim and the accused often reduce the likelihood of obtaining a conviction, the victim's relationships to third parties can similarly reduce the likelihood of conviction.

5. Motives to Fabricate

A motive to fabricate is simply a plausible reason why a victim may make a false allegation.[53] There are many reasons an individual may make a false allegation, the most prevalent of which is to preserve a relationship with a third party.[54] The defense may argue that a victim has a motive to fabricate an allegation if it can establish: 1) that a significant relationship existed with a third party, and 2) that said relationship would be damaged if the victim had consented to sexual activity with the accused. A desire to preserve a relationship with a spouse,[55] a parent,[56] or a boyfriend or girlfriend,[57] have all been held to be of sufficient Sixth Amendment significance to permit defense inquiry and argument.[58] It is not difficult to identify at least one individual within the victim's social sphere that may think less of the victim if the sexual activity were consensual.[59] Therefore, the defense is often able to argue that the sexual act or contact was consensual and that the victim is merely fabricating the allegation before the factfinder.

---

[52] Or that the accused had a mistaken but reasonable belief that the victim consented. Professional Experience, *supra* note 27.
[53] *See* MCM, *supra* note 39, M.R.E. 608(c).
[54] *See* Andre W.E.A. DeZutter et al., *Motives for Filing a False Allegation of Rape*, 47 ARCHIVES OF SEXUAL BEHAVIOR 457, 461 (2017) ("The most frequently reported motivation to file a false allegation of rape was the so-called alibi subcategory," in which a victim utilizes the allegation as a cover for other behavior, such as an extramarital affair.).
[55] United States v. Ellerbrock, 70 M.J. 314, 326 (C.A.A.F. 2011).
[56] United States v. Gaddis, 70 M.J. 248, 251 (C.A.A.F. 2011).
[57] *See* United States v. Collier, Crim. App. No. 200601218 at (C.A.A.F. 2009) (This is a larceny/obstruction of justice case which ruled that the Sixth Amendment right to confrontation permitted inquiry into a homosexual relationship between the accused and the victim).
[58] MCM, *supra* note 39, M.R.E. 412(b)(3).
[59] Sexual Stigmatization is "a sexual double standard within sexuality, where men and women engaging in the same sexual conduct are judged differently—with women carrying the stigma." Pantea Farvid, *Sexual Stigmatization*, ENCYC. OF EVOLUTIONARY PSYCH. SCI. (Jan. 1, 2021), https://link.springer.com/referenceworkentry/10.1007/978-3-319-19650-3_2457.

6. Delayed Reporting

The likelihood of a real-time report of sexual assault is small, as it is common for victims to delay reporting.[60] There is a positive correlation between length of delay and reasonableness of doubt in MSA cases.[61] Moreover, no initial report is perfect. No matter what a victim says or does, their actions will be open to scrutiny and argued through the lens of objective hindsight. The defense will fairly exploit delay, inconsistencies, and any counterintuitive behavior to prevent the Government from meeting the burden.

The common evidentiary problems discussed above exist in nearly every MSA case and, individually or collectively, can preclude proof beyond a reasonable doubt (BARD). Full understanding of MSA in the military justice system requires analyzing the interplay between these common evidentiary shortcomings and the applicable burdens of proof.

D. Burden of Proof

Throughout the criminal process, different burdens of proof apply at various decision points. In MSA cases, the available evidence is often insufficient to obtain a conviction for Article 120 offenses. Statutory, procedural, and evidentiary reforms cannot create evidence that does not exist, which is largely why these changes still do not generate acceptable levels of accountability and deterrence.

---

[60] Emily Pica et al., *The Impact of Delayed Reporting, Assault Type, Victim Gender, and Victim-Defendant Familiarity on Mock-Jurors' Judgments*, 16 APPLIED PSYCH. IN CRIM. JUST. 258, 261 (2022).

[61] *See id.* at 266.

Probable Cause (>40 percent certainty an offense was committed)[62]	Preponderance (>50 percent certainty an offense was committed)[63]	Beyond a Reasonable Doubt (≥96 percent certainty an offense was committed)[64]
1. Searches 2. Preferral 3. Referral 4. Ethical Prosecution	1. Command Investigation Findings of Fact 2. Non-Judicial Punishment 3. Commanding Officer's Substantiation of Misconduct 4. Initial Review Officer's Determination 5. Most Pre-Trial Motions 6. ADSEP/BOI Members' Determination on Substantiation, Separation, and Characterization	Criminal Trial

Fig 1.[65]

[62] Erica Goldberg, *Getting Beyond Intuition in the Probable Cause Inquiry*, 17 LEWIS & CLARK L. REV. 789, 834 (2013) ("Although there is wide variance regarding what [the] percentage is, a significant number of courts and scholars assume that probable cause is within the 40% to 51% range.").

[63] More likely than not. *Preponderance of the Evidence,* CORNELL L. SCH.: LEGAL INFO. INST., https://www.law.cornell.edu/wex/preponderance_of_the_evidence (last visited Apr. 11, 2023).

[64] Jane Goodman-Delahunty & Ryan Essex, *Jury Understanding of Beyond a Reasonable Doubt*, 24 J. OF JUDICIAL ADMIN. 75, 86 (2014). This is an Australian study. There may be slight deviations between an American and Australian quantification of the standard based on culture and other factors; however, this number is a reasonable baseline for assessing the impacts of the constraint imposed by the beyond a reasonable doubt standard (BARD).

[65] Three burdens are applicable in sexual assault cases, probable cause, preponderance, and BARD. Since the focus of this argument is on the delta between probable cause and BARD, preponderance is not addressed.

1. Probable Cause

Probable cause (PC) that a crime was committed plays a vital procedural role in MSA cases. It is the quantum of proof required for military prosecutors to ethically prosecute criminal offenses.[66] It is also the minimum quantum of proof required for a preliminary hearing officer (PHO) and command staff judge advocate (SJA) to recommend referral of a charge.[67] Without PC, a criminal case should never proceed to court-martial. In his 2003 opinion in *Maryland v. Pringle*,[68] Chief Justice Rehnquist attempted to provide clarity on the standard: "[t]he substance of all the definitions of [PC] is a reasonable grounds for belief of guilt."[69] Many courts and scholars estimate PC somewhere between 40 to 51 percent certainty.[70] A 2007 decision from the U.S. Court of Appeals for the Armed Forces clearly articulated in the military context that PC is less than a preponderance.[71] Therefore, military practitioners following precedent understand the PC standard is between 40-50 percent certainty that an offense was committed. The minimum certainty threshold required for a MSA case to proceed to court-martial is the subjective, ambiguous, and low PC burden; the quantum of proof required for a conviction at court-martial is BARD.[72]

2. Beyond a Reasonable Doubt

Although originally proposed by John Adams[73] and subsequently adopted by nearly every criminal jurisdiction, it was not until 1970 that the Supreme Court ruled that proof BARD is required to convict.[74] Similar to the PC standard, American jurisprudence does not provide a precise definition or quantification of BARD. Also contributing to the nebulous

---

[66] U.S. DEP'T OF NAVY, JAGINST 5803.1E, PROFESSIONAL CONDUCT OF ATTORNEYS PRACTICING UNDER THE COGNIZANCE AND SUPERVISION OF THE JUDGE ADVOCATE GENERAL, R. 3.8(a)(1) (20 Jan. 2015) [hereinafter ETHICS].
[67] MCM, *supra* note 39, R.C.M. 405(a).
[68] Maryland v. Pringle, 540 U.S. 366 (2003).
[69] *Id.* at 371 (citation omitted).
[70] Goldberg, *supra* note 62, at 834.
[71] U.S. v. Leedy, 65 M.J. 208, 213 (C.A.A.F. 2007) ("Probable cause requires more than bare suspicion, but something less than a preponderance of the evidence.").
[72] Other standards without significant bearing on sexual assault cases are not addressed in this article (for example, preponderance, clear and convincing, scintilla).
[73] Robert J. McWhirter, *How the Sixth Amendment Guarantees You the Right to a Lawyer, a Fair Trial, and a Chamber Pot*, ARIZ. ATT'Y, Dec. 2007, at 12, 24.
[74] In Re Winship, 397 U.S. 358, 361 (1970).

nature of this concept is each adjudicative body's unique interpretation of the standard in each case.[75] While it is legal error to place a numerical value on the BARD standard in a courtroom, social science has estimated the certainty threshold as high as 96 percent.[76] This quantified level of certainty provides a helpful waypoint to analyze the implications of the burden of proof in MSA cases.

3. Applicable Standards of Proof and Sexual Assault Cases

A military prosecutor must recommend to a convening authority (CA) that cases with less than 40 percent certainty be withdrawn,[77] whereas a prosecutor may ethically prosecute a case that merely meets the PC threshold (40 percent certainty).[78] At an Article 32 preliminary hearing, a PHO will independently assess whether each preferred charge and specification meets the PC threshold.[79] Using the PHO's findings to inform the recommendation, the CA's SJA will also provide an independent assessment as to whether the evidence reaches the PC threshold.[80] A convening authority is not bound by the PC assessment of the prosecutor,[81] PHO, or SJA but generally defers to those assessments.[82]

In many MSA cases, there is sufficient admissible evidence to establish PC, but the admissible evidence is below the BARD threshold. In some cases, the admissible evidence supports a "sufficient certainty window,"[83] meaning despite professional assessments that the evidence is insufficient to establish proof BARD, a reasonable jury could still find the

---

[75] In the civilian context, juries are the adjudicative bodies. *See generally* James A. Shapiro & Karl T. Muth, *Beyond a Reasonable Doubt: Juries Don't Get It*, 52 LOYOLA U. CHI. L. J. 1029 (2021) (explaining that juries are consistently confused by the BARD standard and its application and how jurisdictions manage the standard and its challenges differently).

[76] Goodman-Delahunty & Essex, *supra* note 64, at 86.

[77] *See* ETHICS, *supra* note 66, R. 3.8(a)(1); Goodman-Delahunty & Essex, *supra* note 64, at 86.

[78] *See* ETHICS, *supra* note 66, R. 3.8(a)(1).

[79] MCM, *supra* note 39, R.C.M. 405.

[80] UCMJ art. 34(a)(1) (2022) ("Before referral of charges and specifications to a general court-martial for trial, the convening authority shall submit the matter to the staff judge advocate for advice, which the staff judge advocate shall provide to the convening authority in writing.").

[81] Recent reforms have made a prosecutor's decision binding on a convening authority. National Defense Authorization Act for Fiscal Year 2022, Pub. L. No. 117-81, § 537, 135 Stat. 1541, 1697 (2021).

[82] Professional Experience, *supra* note 27.

[83] For example, a conservative quantification would be equal to or greater than 80 percent certainty.

BARD standard is met. Cases within this window should go to trial. Cases above the PC standard (40 percent certainty) but below a sufficient certainty window (such as an 80 percent certainty), have no reasonable likelihood of obtaining a conviction and should not proceed to court-martial.[84] Referring cases without admissible evidence that exceeds this sufficient certainty window limits future administrative action relative to that accused,[85] does not generate accountability, and provides no deterrent value.

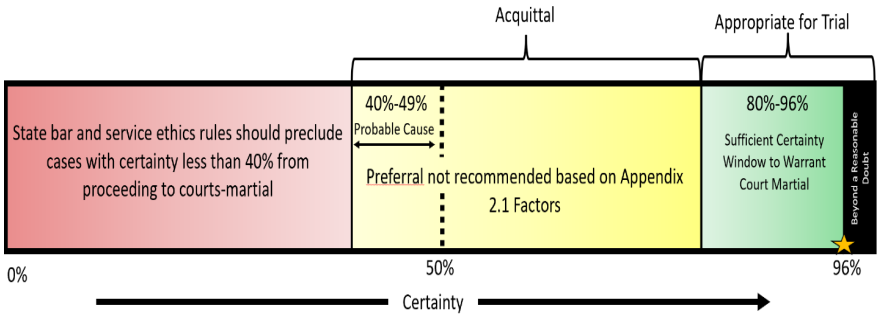

Fig 2.

The delta between PC (40 percent certainty) and BARD (96 percent certainty) is the single greatest contributor to the lack of accountability and deterrence in MSAs.[86] It is relatively easy to reach 40 percent certainty in MSA cases. Identity is rarely an issue and admissions, DNA evidence, or both, often substantiate a sexual contact or act. In theory, merely an allegation by a victim can satisfy the PC standard.

---

[84] *See* MCM, *supra* note 39, app. 2.1, § 2.1(h).

> In determining whether the interests of justice and good order and discipline are served by trial by court-martial or other disposition in a case, the commander or convening authority should consider, in consultation with a judge advocate, . . . [w]hether admissible evidence will likely be sufficient to obtain and sustain a conviction in a trial by court-martial.

MCM, *supra* note 39, app. 2.1, § 2.1(h).

[85] *See e.g.* U.S. MARINE CORPS, ORDER 1900.16 CH. 2, SEPARATION AND RETIREMENT MANUAL para. 6106(1)(a) (15 Feb. 2019) (stating that Marines "may not be separated [for] . . . conduct that has been the subject of military . . . judicial proceedings (including summary court-martial) resulting in an acquittal or action having the effect of acquittal" except for in limited circumstances).

[86] *See* U.S. DEP'T OF JUST., NAT'L INST. JUST., NATIONAL INSTITUTE OF JUSTICE: FIVE THINGS ABOUT DETERRENCE 1-2 (2016) (explaining that the certainty of punishment is a more powerful deterrent to crime than the punishment itself).

By way of example, assume a victim asserts that an accused had non-consensual sexual intercourse with them. Also assume the accused denied the act or invoked the right to remain silent. Absent credibility considerations, the evidence supports a 50 percent likelihood that the crime occurred. This allegation alone exceeds the PC threshold of 40 percent certainty. Under these facts, however, there is no likelihood of obtaining or sustaining a conviction at the BARD threshold. Tweaking the assumptions often yields the same result: assume that the accused admitted to the intercourse (which is corroborated by DNA) but asserted that the victim consented. This case may survive a PC assessment and proceed to trial, but there is a small likelihood of obtaining a conviction. Stacking the ever-present memory issues, pre-existing relationships, motives to fabricate, and delayed reports on top of a case barely at the PC threshold will move the factfinder away from, not towards, BARD. The author's professional experience suggests that these are common scenarios that contribute to current MSA prosecution statistics.[87]

The current MSA conviction rate supports the assertion that the delta between 40 percent certainty and a sufficient certainty window is the primary problem. Former Colorado Attorney General, John Suthers, defined a competent prosecution office as one with a conviction rate between 85-90 percent.[88] The number of preferred cases and percentage of convictions indicate that the military is already over-prosecuting MSAs. This assertion is supported by the findings of the 2020 Defense Advisory Committee Report, which noted that a review of 517 preferred cases from 2017 assessed that 41.2 percent of those cases did not have sufficient admissible evidence to obtain a conviction.[89] Eliminating these 213 cases from the sample set still only yields a conviction rate of 63 percent—far below the benchmark conviction rate of 85-90 percent.[90]

---

[87] Professional experience, *supra* note 27.

[88] JOHN W. SUTHERS, NO HIGHER CALLING, NO GREATER RESPONSIBILITY 82 (2008) ("Overall, a conviction rate of at least 85 to 90 percent (meaning 85-90 percent of all cases filed result in a guilty plea or conviction at trial) would be typical of a competent prosecutor's office.").

[89] DEF. ADVISORY COMM. ON INVESTIGATION, PROSECUTION, AND DEF. OF SEXUAL ASSAULT IN THE ARMED FORCES, REPORT ON INVESTIGATIVE CASE FILE REVIEWS FOR MILITARY ADULT PENETRATIVE SEXUAL OFFENSE CASES CLOSED IN FISCAL YEAR 2017, at 54 (2020) [hereinafter DAC-IPAD].

[90] Percentage means out of 100. *Percent*, MERRIAM-WEBSTER (Apr. 3, 2023), https://www.merriam-webster.com/dictionary/percent. On average, out of any 100 cases in 2017, 6.4 went to trial, 2.6 of those were deemed to have insufficient evidence, 2.4 of those cases resulted in convictions. Therefore, 1.4 of those cases were properly at a court-martial even though there was not a conviction: 2.4 (convictions) / (6.4 (trials) - 2.6 (trials without merit) = 63 percent.

Thus, counsel inexperience, CA prosecutorial discretion, and other military-specific prosecution nuances are not the cause of, nor a significant contributing factor to, the low conviction rate. Many more MSA prosecutions are moving forward than what is merited by accepted prosecution practice, standards, and regulations.[91] In a substantial number of MSA cases, military prosecutors are simply unable to present a sufficient quantum of admissible evidence for a member's panel to determine the Government proved a case BARD. Regardless of the training, education, experience, and resources provided to military prosecutors, previous and present reforms will not appreciably increase convictions in cases without enough evidence. To be clear, the desired goal is not convictions without sufficient evidence, rather the desired end state is to identify actions that should be criminal based on the propensity to cause harm, and then deter and punish those actions.

The filter for cases that reach PC but lack sufficient certainty to merit a court-martial is prosecutorial discretion—historically exercised by general court-martial CAs.[92] Prior to exercising prosecutorial discretion, a CA receives advice from the command's SJA.[93] In the military justice system, SJA advice is informed by a prosecutorial review of the available, admissible evidence and its application to the factors in Appendix 2.1 to the UCMJ.[94] Through those factors, prosecutors analyzing a fact pattern make a non-binding recommendation to the CA, via the SJA, recommending for or against referral.[95] Where a recommendation advises against referral, a CA may close a case, pursue administrative action, or prefer the charges despite the recommendation.[96] Public perception, political pressure, and a desire to pursue justice for victims can detract from the weight of a prosecutor's recommendation in MSA cases.[97] It has been the author's experience that if there is a willing victim and PC, a case will likely go forward.[98] However, referring cases with 40-79 percent

---

[91] *See, e.g.*, U.S. DEP'T OF JUST., JUST. MANUAL §9-27-220 (2023).
[92] Recent reforms will transfer prosecutorial discretion from line officers to senior military prosecutors. National Defense Authorization Act for Fiscal Year 2022, Pub. L. No. 117-81, § 537, 135 Stat. 1541, 1697 (2021).
[93] UCMJ art. 34(a)(1) (2022).
[94] MCM, *supra* note 39, app. 2.1, § 2.1 (including *inter alia*: the views of the victim, the ultimate harm, and whether there is sufficient admissible evidence).
[95] In the Marine Corps, there were, at a minimum, three attorneys behind each case analysis memorandum—a special victim investigation prosecution (SVIP)-qualified counsel, a civilian litigation attorney advisor with significant civilian experience, and the regional trial counsel (an experienced SVIP-qualified attorney serving in an 0-5 billet). Professional Experience, *supra* note 27.
[96] MCM, *supra* note 39, R.C.M. 306.
[97] Professional Experience, *supra* note 27.
[98] Professional Experience, *supra* note 27.

certainty fails to generate justice for victims, does not hold an accused accountable, and siphons resources from cases that merit prosecution. Low conviction rates mean prosecutors are recommending cases proceed that should not, and CAs are referring cases that they should not.[99]

Congress has indicated disapproval with the military's current conviction rate (or batting average[100] for the purposes of the following analogy).[101] Equating cases with 40-79 percent certainty to balls, and cases with greater than 80 percent certainty to strikes, there are not enough good pitches amongst the allegations to generate an acceptable batting average. Any reforms that result in swinging at more bad pitches will not increase the batting average. In the aggregate, previous and proposed reforms have not, and will not, appreciably increase the number of strikes. Providing more resources to batters—training, experts, funding, etc.—will not have a positive impact on the batting average if the batters are still swinging at balls. Even the greatest hitters in the world must be thrown strikes.

E. The Constitution

There are two significant constitutional constraints applicable to all military justice reforms. First, the BARD standard is the constitutionally-required standard at a court-martial.[102] There is good reason for this burden: "The heightened standard of proof in criminal trials is crafted to allocate the risk of error to the state in order to protect the defendant from wrongful conviction."[103] Authorities that wish to avoid this high burden may do so administratively. An administrative separation from the service requires only a preponderance of the evidence (50.1 percent

---

[99] *See* DAC-IPAD, *supra* note 89, at 3; SUTHERS, *supra* note 88, at 82.

[100] In baseball, a batting average, "[o]ne of the oldest and most universal tools to measure a hitter's success at the plate, . . . is determined by dividing a player's hits by his total at-bats." *Batting Average (AVG)*, MLB, https://www.mlb.com/glossary/standard-stats/batting-average (last visited Apr. 11, 2023).

[101] Rebecca Burnett, *U.S. Senate Committee on Armed Services Investigates Sexual Assault in the Military*, DC NEWS NOW (July 8, 2022, 7:20 PM), https://www.dcnewsnow.com/news/local-news/washington-dc/u-s-senate-committee-on-armed-services-investigates-sexual-assault-in-military ("According to Senator Kristen Gillibrand, chair of the United States Senate Committee on Armed Services, U.S. service members are more likely to be sexually assaulted than shot in the line of duty. Sexual assaults have doubled, yet the rate of prosecution and conviction have halved.").

[102] U.S. CONST. art. I, § 8, cl. 5.

[103] Casey Reynolds, *Implicit Bias and the Problem of Certainty in the Criminal Standard of Proof*, 37 L. & PSYCH. REV. 229, 229 (2013).

certainty misconduct was committed).[104] In fact, many cases with proof in the 40-79 percent range would be more adequately addressed via administrative means.[105] Second, an accused must be permitted to put on a defense, meaning they must be allowed to question the Government's witnesses, bring their own witnesses, offer alternative theories, and access evidence that may invade victim privacy, among other rights.[106] Any reform to military justice that does not respect these constitutional requirements is a non-starter.

F. Sex Offense Registration

Sex offense registration is a significant civil disability that limits employment, housing options, and other civil liberties.[107] Convictions for Article 120, UCMJ offenses often require sex offense registration.[108] While the factfinder may not be aware of the specific requirements of sex offense registration, the severity of this collateral consequence is common knowledge. The criminal justice system recognizes the weight sex offender status carries in these cases: "Because of the duration of these requirements, and the stigma attached to the public notification and access to this type of criminal record, the requirement to register for a sexual offense conviction is often one of the most substantial and adversarial parts of the sentence imposed."[109] Given the significance of this collateral consequence, there is a distinct possibility that some panel members may adopt an interpretation of BARD that is more favorable to the accused. If occurring, this is an incorrect application of the burden of proof; however, the phenomenon should be recognized as a potential contributor to low conviction rates in these cases. A low conviction rate and the severe

---

[104] *See, e.g.*, U.S. DEP'T OF ARMY, REG. 15-6, PROCEDURES FOR ADMINISTRATIVE INVESTIGATIONS AND BOARDS OF OFFICERS para. 3-10(b) (1 Apr. 2016); U.S. MARINE CORPS ORDER.1900.16, MARINE CORPS SEPARATIONS MANUAL para. 6319 (15 Feb. 2019).
[105] *See generally* Baker, *supra* note 30.
[106] *See* S. DOC. NO. 103-6, SIXTH AMENDMENT – RIGHTS OF ACCUSED IN CRIMINAL PROSECUTIONS (1992).
[107] Lori McPherson, *The Sex Offender Registration and Notification Act (SORNA) at 10 Years: History, Implementation, and the Future*, 64 DRAKE L. REV. 741, 785-93 (2016).
[108] *Military Convictions Under SORNA*, SMART: OFF. OF SEX OFFENDER SENTENCING, MONITORING, APPREHENDING, REGISTERING, AND TRACKING, https://smart.ojp.gov/sorna/military-convictions (last visited Apr. 12, 2023) ("Title I of the Adam Walsh Child Protection and Safety Act of 2006, the Sex Offender Registration and Notification Act (SORNA), specifically includes certain Uniform Code of Military Justice (UCMJ) convictions in its definition of 'sex offense.'").
[109] MIL. JUST. INT'L, POST COURT-MARTIAL CONVICTION SEX OFFENDER REGISTRATION (n.d.), https://www.militaryjusticeinternational.com/documents/MJISRegBrochure.pdf.

collateral consequence of sex offense registration disincentivizes pleas and encourages defendants to take the case to trial.

G. Problem Statement

How can military justice provide appropriate accountability for, and deterrence of, actions that cause military sexual trauma?

The problem statement is adjudication-agnostic. Regardless of whether an MSA is substantiated, unsubstantiated, or results in a conviction or an acquittal, there are too many individuals (military and civilian) suffering the mental and physical effects of MSA.

III. Effective Strategies

A course of action (COA) must be suitable, feasible, acceptable, and complete.[110] Adapting pre-existing criminal frameworks and extracting portions of successful strategies is a viable starting point for COA development.[111] Two historical COAs provide SAPR components that have the potential to increase accountability and deterrence: The Marine Corps's Bystander Intervention Program[112] and the 6th Marine Corps Recruiting District's (MCD) Operation RESTORE VIGILANCE (RV).[113] Additionally, Articles 120 (Sexual Assault),[114] 128A (Maiming),[115] 130 (Stalking),[116] 133 (Conduct Unbecoming),[117] and 134 (the General Article)[118] provide precedent and inform statutory drafting for criminalizing conduct that can, and should, be adapted as part of a viable approach to MSA reform.

---

[110] *See* MCPP, *supra* note 22, at 3-1. This paper only proposes one COA; the criterion of "distinguishable" has been omitted.
[111] *See* MCPP, *supra* note 22, at 3-2 to 3-3.
[112] *See infra* notes 119-140 and accompanying text.
[113] *See infra* notes 141-164; *see also* Bowers, *supra* note 7.
[114] UCMJ art. 120 (2022) ("Rape and sexual assault generally").
[115] UCMJ art. 128a (2022) ("Maiming").
[116] UCMJ art. 130 (2022) ("Stalking").
[117] UCMJ art. 133 (2022) ("Conduct unbecoming").
[118] UCMJ art. 134 (2022) ("General article").

A. Bystander Intervention

All Marines are required to attend annual sexual assault prevention briefs.[119] The Marine Corps tailors the briefs by audience.[120] The relevant precedent for COA development is the "Step Up"[121] brief for Marines in the E-1 to E-3 ranks and "Take a Stand"[122] brief for Marines in the E-4 to E-5 ranks. "Step Up," has a short education block followed by three vignettes.[123] After the first video, Marine participants are asked to identify warning signs of sexual violence.[124] The second video shows a bystander intervening and preventing sexual assault.[125]

"Take a Stand" training is a three-hour training block for newly promoted Marine non-commissioned officers.[126] The training is approximately three hours and consists of six video segments.[127] In the fourth video segment, "Sexual Assault Prevention," participants are taught to recognize situations with an increased risk of sexual assault. With the aid of video segments, the instructor educates on the techniques that those likely to be accused of sexual assault employ, such as coercion, alcohol, and misuse of authority.[128] During this segment, the facilitator also leads discussion on risk reduction techniques, such as a buddy system and drinking responsibly.[129] Finally, the instructor uses a video and discussion points to reinforce bystander intervention strategies to prevent sexual assault.[130] By the end of the training, all E-1 to E-5 Marines are taught to intervene by directing, distracting, and delegating.[131]

---

[119] *See* DEP'T OF DEF., INSTR. 6495.02, SEXUAL ASSAULT PREVENTION AND RESPONSE PROGRAM PROCEDURES encls. 2, 10 (9 Apr. 2021) [hereinafter DoDI 6495.02]; U.S. MARINE CORPS, ORDER 1752.5C, SEXUAL ASSAULT PREVENTION AND RESPONSE (SAPR) PROGRAM encl. 1, para. 8(a)(b) (3 June 2019).
[120] *See* DoDI 6495.02, *supra* note 119, encl. 10.
[121] Marine Administrative Message, 391/18, R 121650Z July 18, Requirements for Sexual Assault Prevention and Response Training, para. 6.A (12 July 2018) [hereinafter MARADMIN 391/18].
[122] *Id.* para. 6.B; COREEN FARRIS ET AL., MEASURES OF PERFORMANCE AND EFFECTIVENESS FOR THE MARINE CORPS' SEXUAL ASSAULT PREVENTION PROGRAMS 23 (2019).
[123] FARRIS ET AL., *supra* note 122, at 24.
[124] FARRIS ET AL., *supra* note 122, at 24.
[125] FARRIS ET AL., *supra* note 122, at 24.
[126] FARRIS ET AL., *supra* note 122, at 24.
[127] FARRIS ET AL., *supra* note 122, at 25.
[128] FARRIS ET AL., *supra* note 122, at 25.
[129] FARRIS ET AL., *supra* note 122, at 25.
[130] FARRIS ET AL., *supra* note 122, at 25.
[131] U.S. Marine Corps, SAPR Program Overview PowerPoint (n.d.), https://www.mcieast.marines.mil/Portals/33/Documents/Adjutant/3.%20SAPR%20Program%20Overview.ppt.

Directing involves calling out "threatening or inappropriate behavior."[132] This action prevents individuals from being desensitized to these behaviors and stops the escalation of behaviors that can lead to MSA. Distracting requires the bystander to extricate the potential victim from the situation.[133] Delegating involves appointing someone else to help intervene.[134] Marine Corps Community Services asserts that "[b]ystander intervention is one of the most effective ways to interrupt a potential sexual assault."[135] The success of this program depends on the moral courage of third parties to intervene.[136]

"Take a Stand" and "Step Up" are predicated on the existence of objectively verifiable behaviors that lead to MSAs. These behaviors are readily identifiable and collectively referred to as "grooming," which is discussed in detail below.[137] These programs train and implore Marines to intervene when they witness grooming. While these programs have had success,[138] there are some fundamental flaws to this approach. First, the target audience is neither the potential perpetrator nor even the victim. The program attempts to turn a disinterested third party into an interested party despite the lack of a legal duty to intervene. Second, the behaviors bystanders are supposed to intervene and stop are generally not, individually or collectively, criminal.[139] In effect, the Marine Corps asks Marines to run interference on their friends' and colleagues' romantic pursuits to reduce the probability of future sexual misconduct.

If conduct that increases the likelihood of MSA is: 1) objectively identifiable, 2) inappropriate, and 3) worthy of bystander intervention, then it might well be wise to criminalize that conduct in a manner commensurate with the seriousness of the offense to hold the perpetrator accountable. Criminalizing unreasonable sexual pursuit permits commanders to hold an accused accountable for actions that are objectively identifiable, are proven to increase the likelihood of MSA, and

---

[132] MCCS, *Master the Three "D"s of Bystander Intervention*, https://lejeunenewriver.us mc-mccs.org/news/master-the-3-ds-of-bystander-intervention (last visited Apr. 12, 2023) [hereinafter *3Ds*].
[133] *Id.*
[134] *Id.*
[135] *Id.*
[136] *Id.*
[137] *See infra* notes 146-148 and accompanying text.
[138] *3Ds*, *supra* note 132 ("In a recent survey, of the 4 percent of Junior Enlisted respondents who observed a high-risk situation that they believed was or could have led to sexual assault, 86 percent intervened.").
[139] *See 3Ds*, *supra* note 132. There may be some very low-level offenses that would likely never be charged (such as drunk and disorderly, underage drinking) but nothing that compels a preventive blitz by nineteen-year-old bystanders.

are often open and notorious. Criminalizing these behaviors also permits commanders to establish an articulated standard of conduct, train to that standard, and hold bystanders that fail to intervene accountable.[140] From a macro perspective, a statute criminalizing MSA gateway behaviors through a sexual assault lens will help generate accountability and deterrence. While the Bystander Intervention program provides institutional recognition of the precursor behaviors, a case study from the 6th MCD provides a proof of concept.

B. RESTORE VIGILANCE (RV)

From 2008 to 2012, the 6th MCD averaged ten substantiated MSAs per year.[141] In 2012, the 6th MCD promulgated Operation RV, a comprehensive and creative campaign plan aimed at eradicating sexual assault.[142] By 2014, this command of 820 Marines and 7,084 future Marines had no substantiated incidences of recruiter/applicant sexual misconduct.[143] At its core, RV is a command policy targeting the gateway actions to MSA.[144]

RESTORE VIGILANCE's approach to eliminating MSA consisted of four stages: (1) educate stakeholders, (2) attack the conditions that permit sexual misconduct, (3) shield the vulnerable population, and (4) create a culture of accountability.[145] Stage (2) is particularly relevant to the proposed military justice reform: "Wage an all-out 'war' against the conditions in which sexual misconduct can occur."[146] Additionally, Stage (2) consisted of three specific tactics that eliminated or degraded identified precursors to recruiter/applicant sexual misconduct—isolation, texting, and normalizing[147] (in other words, "grooming").

Grooming in the context of MSA, consists of the "manipulative behaviors that the abuser uses to gain access to a potential victim, coerce

---

[140] *See* U.S. DEP'T OF NAVY, U.S. NAVY REGULATIONS art. 1137 (1990) ("Persons in the naval service shall report as soon as possible to superior authority all offenses under the Uniform Code of Military Justice which come under their observation. . . .").
[141] Bowers, *supra* note 7, at 1.
[142] U.S. MARINE CORPS, CAMPAIGN PLAN 01-03, 6TH MCD OPERATION "RESTORE VIGILANCE" CAMPAIGN PLAN (18 Sept. 2012) [hereinafter CP 01-03].
[143] Bowers, *supra* note 7, at 4. There was one instance of sexual misconduct—a consensual sexual relationship between a recruiter and a poolee. Bowers, *supra* note 7, at 4.
[144] *See* Bowers, *supra* note 7, at 1.
[145] Bowers, *supra* note 7, at 1-4.
[146] Bowers, *supra* note 7, at 2.
[147] Bowers, *supra* note 7, at 2.

them to agree to the abuse, and/or reduce the risk of being caught."[148] These behaviors include, but are not limited to: (1) "[g]aining access and isolating the victim," (2) victim selection, (3) "[t]rust development and keeping secrets," (4) "[d]esensitization to touch and discussion of sexual topics," and (5) "[a]ttempts by abusers to make their behavior seem natural."[149] Without compromising the mission and in a legally permissible manner, 6th MCD effectively eliminated the ability to isolate a victim and significantly degraded potential offenders' ability to execute the remaining behaviors.

To combat the ability for potential offenders to isolate victims, the command instituted a "Two-Person Integrity" (TPI) policy requiring two recruiters during contact with an applicant.[150] Exceptions to the TPI policy required waivers, additional oversight, and follow-up.[151] With the policy in place, the commander could hold violators administratively or criminally accountable for simply being in a one-on-one situation.[152] Flanking the problem from the other side of the equation, the TPI policy deters sexual misconduct by educating applicants, enabling them to recognize and report violations of the policy, and establishing direct command liaison. This strategy holds potential perpetrators at punitive risk. No recruiter could effectively insulate from the risk that the command would become aware of a TPI violation. The TPI policy was a masterstroke that eliminated a necessary tool of sexual predators—isolation.

To degrade recruiters' ability to groom via behaviors (2)-(5) above, the 6th MCD banned "all forms of communication on personal devices between Marines and applicants."[153] This measure specifically targeted texting.[154] The 6th MCD recognized, "texting is an unsupervised, informal, and dangerous mode of communication that can easily be misunderstood and manipulated by predators."[155] During the course of text message conversations in MSA situations, offenders can probe to assess boundaries, hide behind ambiguity, maintain engagement, and can communicate things that are not socially acceptable via other communication methods. Without the ability to privately text with applicants, it becomes exponentially more difficult for potential offenders

---

[148] *Grooming: Know the Warning Signs*, RAINN (July 10, 2020), https://www.rainn.org/news/grooming-know-warning-signs.
[149] *Id.*
[150] Bowers, *supra* note 7, at 2.
[151] CP 01-03, *supra* note 142, para. 3(b)(2)(a).
[152] *See infra* notes 177-179 and accompanying text.
[153] Bowers, *supra* note 7, at 2.
[154] Bowers, *supra* note 7, at 2.
[155] Bowers, *supra* note 7, at 2.

to: (2) effectively select a victim, (3) develop the type of trust required, (4) desensitize the victim to discussion of sexual topics, and (5) normalize a potential perpetrator's behavior.

The 6th MCD also targeted behavior normalization by tasking the command with identifying and stopping "inappropriate language, dress, and juvenile behavior."[156] The 6th MCD identified that potential sexual predators were often "narcissistic, sociopathic, hyper-masculine," and violent.[157] By recognizing these character traits, the 6th MCD was able to prevent introduction of those inappropriate behaviors into the environment. Without the ability to introduce and exploit these behaviors, potential predators were unable to pollute the environment and desensitize subordinates, peers, superiors, and victims to behavior consistent with sexual predators.[158]

While there were no sexual misconduct allegations within the 6th MCD in 2014, nine Marines were relieved for violating RV policies.[159] Of the nine that were relieved:

> [two] Marines . . . [were] communicating with female applicants on their personal devices; three Marines . . . [were] inviting Marines to their personal residences to consume alcohol; one Marine . . . [was] communicating with a female applicant in an unprofessional manner on social media; one Marine . . . [was] violating a military protective order with a female applicant; and two Marines . . . [were] violating the TPI policy.[160]

Proving a negative is impossible. However, ten instances of sexual misconduct per year reduced to zero, coupled with the nine Marines relieved for violating RV policies, indicates that the 6th MCD identified and implemented a viable approach to preventing MSA. One can infer that some of those relieved were on a path to unwelcome sexual conduct.[161] The commanding officer of the 6th MCD recognized that the lack of sexual misconduct "does not necessarily mean that 6th MCD had no sexual predators within [its] ranks";[162] however, the lack of reported crimes does

---

[156] Bowers, *supra* note 7, at 2.
[157] Bowers, *supra* note 7, at 5.
[158] Bowers, *supra* note 7, at 2.
[159] Bowers, *supra* note 7, at 2.
[160] Bowers, *supra* note 7, at 4.
[161] *See* Bowers, *supra* note 7, at 4 ("It is my belief that at least some of these Marines were on the trajectory towards committing an act of sexual misconduct—to include possibly assault—against some of our future Marines.").
[162] Bowers, *supra* note 7, at 4.

indicate that the 6th MCD was outpacing and outmaneuvering them. While the relieved Marines' careers were jeopardized, within the 6th MCD, there were no victims of MSA, there were no MSA courts-martial, there were no MSA convictions, and no Marines were required to register as sex offenders. From an accountability and deterrence perspective, the end state achieved by the 6th MCD is an end state that should satisfy all stakeholders.

The success of this program begs the question: "Why has this campaign plan not been implemented throughout the DoD?" Unfortunately, RV is not plug-and-play.[163] The unique relationship between a recruiter and an applicant affords recruiting district commanding officers more latitude to regulate Service member conduct than is currently afforded commanding officers in other contexts.[164] However, RV offers a valuable proof-of-concept were commanders in other contexts provided similar tools.

C. Existing Precedent from Law and Statute

Bystander intervention and RV inform the tactics and efficacy of addressing precursor behaviors to MSA. Existing precedent, statutes, and discussion provide vetted language, definitions, and strategies that can be adapted to provide an additional tool to combat MSA through Article 134, UCMJ. Article 120 provides the necessary definitions for "sexual act" and "sexual contact."[165] Language from Article 130, stalking, can be adopted to criminalize a course of conduct—the necessary continuity of purpose being the intent to commit a sexual act or contact.[166] Article 133, conduct unbecoming an officer, enables the military to define an acceptable standard of conduct for a class of Service members (such as officers) and criminalize acts and omissions that fail to meet that standard.[167] Some criminal statutes permit the ultimate harm to serve as proof of intent to commit a crime.[168] Finally, and importantly, criminalizing precursor behaviors to MSA is unconstitutional absent a military nexus, since these behaviors are not criminal in other contexts. The use of Article 134 to

---

[163] *See* Gregg Curley, *New Ideas to Prevent Sexual Assault in the Military*, 148 PROCEEDINGS 1430 (2022).
[164] *See, e.g.*, U.S. DEP'T OF ARMY, REG. 600-20, ARMY COMMAND POLICY para. 4-15(b) (24 July 2020) (delineating specific actions that are prohibited "between recruiters and prospects, applicants, and/or recruits").
[165] UCMJ art. 120 (2022).
[166] UCMJ art. 130 (2022).
[167] UCMJ art. 133 (2022).
[168] *See* UCMJ art. 128a (2022).

criminalize this conduct provides the mechanism for ensuring the military nexus and, therefore, the constitutionality of the crime.[169]

D. Proposed Course of Action: Criminalize Precursor Behaviors to Sexual Assault

Criminalization of precursor behaviors can be accomplished with four elements: (1) That the accused wrongfully engaged in a course of conduct directed at a specific person;[170] (2) The course of conduct [was intended to] [did] result in a sexual contact or sexual act as described in section 920(g) of this title (article 120(g));[171] (3) That, under the circumstances, the course of conduct was unreasonable; and, (4) That, under the circumstances, the conduct of the accused was either: (a) to the prejudice of good order and discipline in the armed forces; (b) was of a nature to bring discredit upon the armed forces; or (c) to the prejudice of good order and discipline in the armed forces and of a nature to bring discredit upon the armed forces.

This proposed COA addresses multiple problems inherent in the current MSA framework. First, it permits criminal liability for MSA while eliminating questions of consent or mistake of fact. Second, the proposed statute recognizes evidentiary limitations and addresses provable conduct. Third, it enables criminalization of conduct that occurs prior to the MSA and often has corroborating witnesses and evidence. Fourth, the proposed statutory language targets non-registerable conduct.

---

[169] UCMJ art. 134 (2022). The text of Article 134 reads:

> Though not specifically mentioned in this chapter, all disorders and neglects to the prejudice of good order and discipline in the armed forces, all conduct of a nature to bring discredit upon the armed forces, and crimes and offenses not capital, of which persons subject to this chapter may be guilty, shall be taken cognizance of by a general, special, or summary court-martial, according to the nature and degree of the offense, and shall be punished at the discretion of that court. As used in the preceding sentence, the term "crimes and offenses not capital" includes any conduct engaged in outside the United States, as defined in section 5 of title 18, that would constitute a crime or offense not capital if the conduct had been engaged in within the special maritime and territorial jurisdiction of the United States, as defined in section 7 of title 18.

Id.

[170] *See* UCMJ art. 130 (2022) ("Stalking"); MCM, *supra* note 39, pt. IV, ¶ 80.

[171] UCMJ art. 120 (2022) ("Rape and sexual assault generally"); MCM, *supra* note 39, pt. IV, ¶ 60.

Therefore, the associated punishments and lack of sex offense registration will remove an incentive for the defense to try the case. Last, this offense will increase MSA accountability and deterrence.

1. Benefits to the Proposed Crime of Exploitation

Every category of stakeholder stands to gain from an exploitation framework. The proposal provides more adjudication options for victims. An accused may plead to a substantial MSA-related offense that does not require sex offense registration. Prosecutors would be armed with a criminal framework that, in many cases, is more likely to obtain a conviction. The crime furnishes the accountability and deterrence that Congress seeks.[172] It affords a means for CAs to remove sexual predators from the ranks. It provides SAPR professionals standards to which they can train. As is, an accused facing MSA charges often weighs the likelihood of two outcomes: felony conviction (requiring sex offense registration and a punitive discharge) or acquittal. Exploitation would prevent misconduct from slipping through the current all-or-nothing MSA paradigm while capping punishment at a level commensurate with the offense.

2. Drawbacks to the Proposed Crime of Exploitation

Certainly, there are drawbacks to the proposed crime. First, there is a perception that Congress has already over-criminalized MSA. Until 2007, MSA was absent from the UCMJ.[173] Now, the MCM contains pages of statutes, and there are volumes of case law on the subject.[174] However, the proposed crime is not targeting sexual conduct *per se*, but rather the gateway actions—those things a Service member does or fails to do that enable them to "take advantage" of a victim.

Under this proposal, Service members remain free to pursue sexual gratification. It is only when that pursuit of sexual gratification falls below the standard of conduct expected of a Service member that the actions become criminal. The gravamen of this crime is the course of conduct vice

---

[172] *See, e.g.*, Michel Paradis, *Congress Demands Accountability for Service Members*, LAWFARE (June 1, 2021, 9:28 AM), https://www.lawfareblog.com/congress-demands-accountability-service-members.

[173] *See* National Defense Authorization Act for Fiscal Year 2006, Pub. L. No. 109-163, §552, 119 Stat. 3136, 3256 (2006) (revising Article 120 to include sexual assault).

[174] *See* MCM, *supra* note 39, pt. IV, ¶ 60.

the ultimate sexual act; therefore, registration is not appropriate based solely on a conviction for this charge. The lack of a registration requirement for this misconduct is an appropriate outcome.

Lastly, there will likely be constitutional challenges to the proposed crime (e.g., void for vagueness, notice, or overbreadth). However, there is no reason to fear challenges if the language is appropriately drafted, Service members are provided adequate notice of the applicable standard of conduct, and the crime is properly charged. There is already established precedent from other presidentially-prescribed Article 134 crimes that have already survived these constitutional challenges.

IV. COA Implementation

There are four practical ways that courses of conduct preceding an MSA allegation may be criminalized. First, Congress can pass a statute criminalizing the conduct. Second, service secretaries or subordinate flag commanders can issue general orders prohibiting the conduct. Third, the General Article may be used to criminalize conduct on a case-by-case basis.[175] The fourth, and most effective and appropriate method of criminalization, is for the President to proscribe the misconduct under an enumerated Article 134 chapter.

The most obvious way to criminalize conduct is to do so via an enumerated statute. However, enumerated articles do not require a military nexus[176]—an important component in criminalizing exploitation. Senior flag officers and service secretaries can regulate behavior, even otherwise lawful personal behavior, if there is a specific military purpose for doing so.[177] There are multiple reasons why promulgating orders is not the appropriate manner to criminalize exploitation. First, there would be disparate policies across the services. Second, much of the individual conduct at issue is otherwise legal—it is: 1) the articulated standard of conduct, 2) the intent accompanying the acts, and 3) the military nexus that would render this otherwise-legal conduct unlawful. Taking legal behavior and making it illegal can certainly be accomplished via orders—

---

[175] UCMJ art. 134 (2022).
[176] *See, e.g.*, UCMJ art. 130 (2022).
[177] *See* U.S. v. Moore, 58 M.J. 466, 467-68 (2003); DAVID A. SCHLUETER, MILITARY CRIMINAL JUSTICE: PRACTICE AND PROCEDURE § 2-4(C) (8th ed. 2012) [hereinafter, PRACTICE AND PROCEDURE].

for example, the possession of drug paraphernalia[178] or using lawful products for unlawful purposes (such as huffing).[179] However, those behaviors do not have constitutional implications. Individual commanders issuing orders banning exploitation will lead to confusion, notice issues, and sub-optimal results.

The General Article can render conduct criminal even if it is not specifically criminalized by Congress—it is a catch-all punitive article.[180] The General Article has existed in military criminal law, in some form, since the Revolution[181] and because of due process concerns and *ex post facto* issues,[182] is a broad grant of power that is constitutional only in the military context.[183] The same equities that render the catch-all provision constitutional justify enhanced regulation and criminalization of exploitation—specifically, the impact MSA has on good order and discipline, morale, esprit de corps, and national defense.[184]

While Article 134 is facially broad and vests prosecutors with the ability to "invent" crimes, there are limits to what prosecutors can attempt to criminalize under this article[185]—and limited returns to the effort, since different judges and commanders will be variably receptive to the approach. Conduct must directly affect good order and discipline or have the potential to damage the reputation of the service.[186] The proposed criminal language proscribes conduct that would otherwise be legal, although morally questionable. Therefore, any General Article charge would require a factual showing of the conduct's deleterious impact on good order and discipline.[187] If conduct is not prejudicial to good order and discipline, it can still bring discredit on the service—"lowering the civilian community's esteem or bringing the armed forces into

---

[178] *See, e.g.*, Headquarters, U.S. South Command, Gen. Order No. 1 (22 Feb. 2021) ("Prohibited Activities for Personnel within the United States Southern Command (USSOUTHCOM) Area of Responsibility (AOR)").

[179] *See, e.g.,* Memorandum from Commanding Gen., Headquarters, Joint Readiness Training Ctr. And Fort Polk, Subject: Joint Readiness Training Center (JRTC) and Fort Polk Policy 12 – Prohibiting Possession of Drug Paraphernalia and Inhalant Abuse paras. 7(a), 8 (12 Apr. 2022) (declaring that huffing is prohibited and that "[t]his policy memorandum constitutes a lawful general order issued under my authority as a General Court-Martial Convening Authority").

[180] PRACTICE AND PROCEDURE, *supra* note 177, § 2-6(A).

[181] DAVID A. SCHLUETER ET AL., MILITARY CRIMES AND DEFENSES § 7.3 (3d ed. 2020) [hereinafter MILITARY CRIMES AND DEFENSES].

[182] *Id.* § 7.1.

[183] *See* Parker v. Levy, 417 U.S. 733, 756 (1974).

[184] *See* MCM, *supra* note 39, pt. IV, ¶ 91(c).

[185] *See* MILITARY CRIMES AND DEFENSES, *supra* note 181, § 7.1.

[186] PRACTICE AND PROCEDURE, *supra* note 177, §§ 2-6(B), (C).

[187] United States v. Poole, 39 M.J. 819, 821 (A.C.M.R. 1994).

disrepute."[188] Of course, the conduct can be both prejudicial to good order and discipline and service-discrediting.[189] The greatest bar, however, to utilizing the General Article is the notification requirement.

For an Article 134 offense to be constitutional, an accused must have fair notice that the conduct is chargeable as a violation of Article 134, as well as notice of the standard applicable to the forbidden conduct.[190] Criminalizing exploitation via the General Article will fail in this regard. Without a defined standard, individual prosecutors could charge the course of conduct in an ad hoc fashion and accused Service members would not have knowledge of the standard. Localized orders could proscribe the conduct and articulate the standard, but charging localized orders should be done via Article 92, UCMJ vice as a violation of the General Article.[191] The Court of Appeals for the Armed Forces has determined that notice of the criminal conduct can come from "the [MCM], federal law, state law, military case law, military custom and usage, and military regulations."[192] To render the standard universally applicable across the service and notify the entire force, a presidentially-proscribed Article 134 crime is the appropriate mechanism for criminalization.

Following the General Article in the MCM, there are sixteen enumerated crimes under Article 134.[193] These crimes still fall under the General Article, but the President has exercised authority under Article 36, UCMJ to provide clarity and notice by defining elements, maximum punishments, and model specifications for common disorders and neglects.[194] Presidentially-articulated crimes under the General Article

---

[188] PRACTICE AND PROCEDURE, *supra* note 177, § 2-6(C).
[189] MCM, *supra* note 39, pt. IV, ¶ 91(c)(6)(a).
[190] MILITARY CRIMES AND DEFENSES, *supra* note 181, § 7.3[3][c][i].
[191] *See* UCMJ, art. 92 (2022) ("Failure to obey order or regulation.").
[192] MILITARY CRIMES AND DEFENSES, *supra* note 181, § 7.3[3][c][i] (citing United States v. Vaughan, 58 M.J. 29, 31 (C.A.A.F. 2003)).
[193] MCM, *supra* note 39, pt. IV, ¶¶ 92-108 (including straggling, dishonorably failing to pay debts, and child pornography). In addition, in January 2022, President Biden signed an executive order making sexual harassment an offense under Article 134 of the UCMJ. Exec. Order No. 14062, 87 Fed. Reg. 4763 (Jan. 31, 2022).
[194] UCMJ art. 36 (2022).

> Pretrial, trial, and post-trial procedures, including modes of proof, for cases arising under this chapter triable in courts-martial, military commissions and other military tribunals, and procedures for courts of inquiry, may be prescribed by the President by regulations which shall, so far as he considers practicable, apply the principles of law and the rules of evidence generally recognized in the trial of criminal cases in the United States district courts, but which may not, except as provided

ensure enumerated crimes under Article 134 are not constitutionally overbroad:

> Each article has been construed . . . so as to limit its scope, thus narrowing the very broad reach of the literal language of the articles, and at the same time supplying considerable specificity by way of examples of the conduct that they cover.[195]

Presidential language will accomplish four things. First, it will articulate to the entire force a legally enforceable standard of conduct (see Appendix A). Second, presidential language included in the MCM will satisfy the requirement of placing every military member on notice of the criminal conduct. Third, the President may set the maximum punishments. Fourth, presidentially-proscribed Article 134 crimes require a military nexus. This nexus is vital to ensure that behavior, which may have constitutional implications in the civilian context, can be properly regulated in the military context.

V. Maximum Punishments

Individuals charged with and convicted of exploitation are guilty of unreasonable advances towards potential sexual partners that are prejudicial to good order and discipline or service discrediting. In other words, the actions in pursuit of sexual gratification fell below the standards expected of members of the military.[196] The maximum punishments associated with the crime should correlate to the ultimate harm of the crime. Exploitation that does not result in a sexual act or a sexual contact, should have a low maximum punishment.[197] Even the most egregious cases that lack physical contact should not exceed the summary court-martial sentence limitations. This punishment scheme

---

> in chapter 47A of this title, be contrary to or inconsistent with this chapter.

Id. art. 36(a).

[195] MILITARY CRIMES AND DEFENSES, *supra* note 181, § 7.3.

[196] *See* UCMJ art. 133 (2022) ("Conduct unbecoming an officer"). See MCM, *supra* note 39, pt. IV, ¶ 90 for an articulated standard of conduct. The President would have to do the same for this proposed statute and make it applicable to all Service members.

[197] The author recommends thirty days' confinement with no punitive discharge is an appropriate maximum punishment.

will ensure that most exploitation cases without contact, which are minor infractions, are adjudicated via non-judicial punishment, administrative separation, summary courts-martial, or counseling—an appropriate level given the ultimate harm and nature of the crime. Exploitation resulting in sexual contact or sexual act(s) leads to far greater harm than an exploitation without contact. An individual convicted of these subclasses of the crime has exhibited behaviors associated with sexual predation and should face a larger quantum of punishment.[198] A more severe punishment framework for contact cases permits flexibility when the sentencing authority applies the facts to the law and sentencing factors, but can also permit or mandate a punitive discharge where appropriate. The sentencing scheme in these cases should strike a balance between meriting or requiring a punitive discharge with recognition that this crime is not sexual assault, but rather, pursuit of sexual gratification that falls below military community standards.

VI. Conclusion

"Left of bang," military justice only contributes to MSA prevention via deterrence. "Right of bang," military justice is a mechanism to provide accountability for MSA. If Congress, DoD leaders, and commanders want to reduce MSAs and correlated military sexual trauma, targeting precursor behaviors via training and appropriate criminal liability is an effective means of doing so. Exploitation holistically and effectively targets the precursor behaviors, thereby increasing deterrence of, and accountability for, MSA. The proposed statute can pass constitutional muster, does not radically change the military justice system, provides a relief valve for victims and the accused, and provides measured justice for accused Service members.

---

[198] The author recommends six months' confinement and a bad conduct discharge for "sexual contact" and twelve months' confinement and a mandatory bad conduct discharge for "sexual act."

Appendix A: Proposed 134 Presidential Language

99. Article 134—(Exploitation)

a. *Text of statute*. See paragraph 91.

b. *Elements*.

(1) *Exploitation*.

(a) That the accused wrongfully engaged in a course of conduct directed at a specific person;[199]

(b) The course of conduct was intended to result in a sexual contact or sexual act as described in section 920(g) of this title (article 120(g));[200]

(c) That, under the circumstances, the course of conduct was unreasonable; and,

(d) That, under the circumstances, the conduct of the accused was either:

(i) to the prejudice of good order and discipline in the armed forces;

(ii) was of a nature to bring discredit upon the armed forces; or

(iii) to the prejudice of good order and discipline in the armed forces and of a nature to bring discredit upon the armed forces.

(2) *Exploitation resulting in sexual contact*.

(a) That the accused wrongfully engaged in a course of conduct directed at a specific person;[201]

---

[199] *See* UCMJ art. 130 (2022) ("Stalking"); MCM, *supra* note 39, pt. IV, ¶ 80.
[200] UCMJ art. 120 (2022) ("Rape and sexual assault generally"); MCM, *supra* note 39, pt. IV, ¶ 60.
[201] *See* UCMJ art. 130 (2022) ("Stalking"); MCM, *supra* note 39, pt. IV, ¶ 80.

(b) The course of conduct was intended to result in a sexual contact or sexual act as described in section 920(g) of this title (article 120(g));[202]

(c) That, under the circumstances, the course of conduct was unreasonable;

(d) The conduct resulted in a sexual contact as described in section 920(g) of this title (article 120(g)).[203]

(e) That, under the circumstances, the conduct of the accused was either:

(i) to the prejudice of good order and discipline in the armed forces;

(ii) was of a nature to bring discredit upon the armed forces; or

(iii) to the prejudice of good order and discipline in the armed forces and of a nature to bring discredit upon the armed forces.

(3) *Exploitation resulting in a sexual act*.

(a) That the accused wrongfully engaged in a course of conduct directed at a specific person;[204]

(b) The course of conduct was intended to result in a sexual contact or sexual act as described in section 920(g) of this title (article 120(g));[205]

(c) That, under the circumstances, the course of conduct was unreasonable;

(d) The conduct resulted in a sexual act as defined in section 920(g) of this title (article 120(g)).[206]

---

[202] UCMJ art. 120 (2022) ("Rape and sexual assault generally"); MCM, *supra* note 39, pt. IV, ¶ 60.
[203] UCMJ art. 120 (2022) ("Rape and sexual assault generally"); MCM, *supra* note 39, pt. IV, ¶ 60.
[204] *See* UCMJ art. 130 (2022) ("Stalking"); MCM, *supra* note 39, pt. IV, ¶ 80.
[205] UCMJ art. 120 (2022) ("Rape and sexual assault generally"); MCM, *supra* note 39, pt. IV, ¶ 60.
[206] UCMJ art. 120 (2022) ("Rape and sexual assault generally"); MCM, *supra* note 39, pt. IV, ¶ 60.

(e) That, under the circumstances, the conduct of the accused was either:

(i) to the prejudice of good order and discipline in the armed forces;

(ii) was of a nature to bring discredit upon the armed forces; or

(iii) to the prejudice of good order and discipline in the armed forces and of a nature to bring discredit upon the armed forces.

c. *Explanation*.

(1) The term "conduct" means conduct of any kind, including but not limited to, isolating an individual; persisting despite affirmative lack of consent to the conduct; underage or excessive alcohol consumption; use of illegal substances; orders violations; violations of customs of the service; providing alcohol or other illegal substances; gaining access; setting conditions to permit access; encouraging unlawful conduct; exerting pressure from rank, status, or billet; and violations of other statutes, rules, regulations.

(2) The term "course of conduct" means—

(a) a pattern of conduct composed of repeated acts evidencing a continuity of purpose;

(b) Unreasonable re-engagement without a sufficient lapse of time or cooling off period;[207] or,

(c) Continuing interaction beyond the point at which continued interaction with the individual is not objectively reasonable.

(3) This paragraph prohibits courses of conduct which seriously compromise the Service member's character, or action, or behavior in an unofficial or private capacity which, in dishonoring or disgracing the Service member, seriously compromises the person's standing as a member of the Armed Forces. There are certain moral attributes common to the ideal Service member, a lack of which is indicated by acts of dishonesty, harassment, unfair dealing, indecency, indecorum, lawlessness, injustice, maltreatment, or cruelty. Not everyone is or can be

[207] *See*, Maryland v. Shatzer, 559 U.S. 98, 124 n.7 (2010) (discussing reengaging with counsel, where factors considered included the amount of time to re-acclimate to normal life, consult with friends and counsel, and shake off residual effects of prior custody).

expected to meet unrealistically high moral standards, but there is a limit of tolerance based on customs of the Service and military necessity, below which the personal standards of a Service member cannot fall without seriously compromising the person's standing as Service member or the person's character as a Service member. This Article prohibits courses of conduct, by Service members, with the aim of resulting in sexual conduct, which, taking all the circumstances into consideration, is thus compromising.[208]

(4) *Exploitation as a separate offense*. Exploitation is a separate and distinct offense from a sexual assault, and both the exploitation and the consummated offense that was its object may be charged, tried, and punished. The commission of the intended offense may satisfy the intent element of the exploitation charge.

(5) Conduct prejudicial to good order and discipline or of a nature to bring discredit upon the armed forces. To constitute an offense under the UCMJ, the exploitation must either be directly prejudicial to good order and discipline or service discrediting, or both. Exploitation that is directly prejudicial to good order and discipline includes conduct that has an obvious and measurably divisive effect on unit or organization discipline, morale, or cohesion, or is clearly detrimental to the authority or stature of or respect toward a Service member, or both. Exploitation may be service discrediting, even though the conduct is only indirectly or remotely prejudicial to good order and discipline. "Discredit" means to injure the reputation of the armed forces and includes exploitation that has a tendency, because of its open or notorious nature, to bring the service into disrepute, make it subject to public ridicule, or lower it in public esteem. While exploitation that is private and discreet in nature may not be service discrediting by this standard, under the circumstances, it may be determined to be conduct prejudicial to good order and discipline. All relevant circumstances, including but not limited to the following factors, should be considered when determining whether exploitation is prejudicial to good order and discipline or is of a nature to bring discredit upon the armed forces, or both:

(a) The accused's marital status, military rank, grade, or position;

(b) The victim's marital status, military rank, grade, and position, or relationship to the armed forces;

---

[208] *See* UCMJ art. 133 ("Conduct unbecoming an officer and a gentleman"); MCM, *supra* note 39, pt. IV, ¶ 90.

(c) The military status of the accused's spouse or the spouse of the victim, or their relationship to the armed forces;

(d) The impact, if any, of the course of conduct on the ability of the accused or the victim or the spouse of either to perform their duties in support of the armed forces;

(e) The negative impact of the course of conduct on the unit or organization of the accused, or the victim, such as a detrimental effect on unit or organization morale, operational readiness, teamwork, loss of trust, efficiency, or reputation;

(f) The misuse, if any, of Government time and resources to facilitate the course of the conduct; and,

(g) The flagrancy of the course of conduct, such as whether any notoriety ensued; and whether the course of conduct included other violations of the UCMJ.

d. Maximum punishment.

(1) *Exploitation.* Confinement for 1 month and forfeiture of two-thirds pay per month for 1 month.

(2) *Exploitation resulting in a sexual contact.* Confinement for 6 months, forfeiture of two-thirds pay per month for 6 months and a bad conduct discharge.

(3) *Exploitation resulting in a sexual act.* Confinement for 12 months and forfeiture of two-thirds pay per month for 12 months. Mandatory minimum dismissal or bad conduct discharge.

e. Sample specification.

(1) *Exploitation.*

In that _____ (personal jurisdiction data), did (at/on board—location) (subject-matter jurisdiction, if required), (on or about _____ 20 __) (from about _____ to about _____ 20 __), with the intent to engage in a (sexual act) (sexual contact), wrongfully engage in a course of conduct to wit:_____ directed at _____, after a reasonable person would have ceased said conduct, and that said conduct was (to the prejudice of good order and discipline in the armed forces) (of a nature to bring discredit upon the armed forces) (to the prejudice of good order and discipline in the armed forces and was of a nature to bring discredit upon the armed forces).

(2) *Exploitation resulting in sexual contact.*

In that _____ (personal jurisdiction data), did (at/on board—location) (subject-matter jurisdiction, if required), (on or about _____ 20 __) (from about _____ to about _____ 20 __), with the intent to engage in a (sexual act) (sexual contact), wrongfully engage in a course of conduct, to wit:_____ directed at _____, after a reasonable person would have ceased said conduct, the course of conduct resulted in (a sexual contact)(sexual contacts), and that said conduct was (to the prejudice of good order and discipline in the armed forces) (of a nature to bring discredit upon the armed forces) (to the prejudice of good order and discipline in the armed forces and was of a nature to bring discredit upon the armed forces).

(3) *Exploitation resulting in sexual act.*

In that _____ (personal jurisdiction data), did (at/on board—location) (subject-matter jurisdiction, if required), (on or about _____ 20 __) (from about _____ to about _____ 20 __), with the intent to engage in a (sexual act) (sexual contact), wrongfully engage in a course of conduct to wit:_____ directed at _____, after a reasonable person would have ceased said conduct, the course of conduct resulted in (a sexual act)(sexual acts)(sexual contacts and sexual acts), and that said conduct was (to the prejudice of good order and discipline in the armed forces) (of a nature to bring discredit upon the armed forces) (to the prejudice of good order and discipline in the armed forces and was of a nature to bring discredit upon the armed forces).

GIVING THE CYBERSECURITY MATURITY MODEL CERTIFICATION TEETH: ENSURING COMPLIANCE IN CONTRACTOR SELF-CERTIFICATIONS

MAJOR THOMAS J. HOESMAN*

I. Introduction

In early 2018, the Chinese Ministry of State Security obtained 614 gigabytes of data from a contractor working for the Naval Undersea Warfare Center by compromising its unclassified electronic information storage systems.[1] The contents of the breach, while unclassified,[2] were sensitive enough that the Department of Defense (DoD) declined to disclose even the specific nature of the contract,[3] and the news outlet that broke the story agreed to withhold certain information it had uncovered because of its potential to "harm national security."[4] As noted at the time, "hundreds of mechanical and software systems [concerning undersea warfare] were compromised—a significant breach in a critical area of warfare that China has identified as a priority, both for building its own capabilities and challenging those of the United States."[5] This loss of non-public but unclassified information related to the contractor's project "deeply reduce[d] [the DoD's] level of comfort if [it] were in a close

* Judge Advocate, United States Air Force. Presently assigned as Acquisition Counsel, Air Force Materiel Command, Wright-Patterson Air Force Base, Ohio. LL.M., 2022, The Judge Advocate General's Legal Center and School, U.S. Army; J.D., 2015, University of Maryland Francis King Carey School of Law; B.A., 2012, St. Mary's College of Maryland. Previous assignments include Area Defense Counsel, Trial Defense Division, Vandenberg Space Force Base, California, 2019–2021; Chief of Administrative Law and Trial Counsel, 30th Space Wing, Vandenberg Air Force Base, 2016-2019. Member of the Bars of Maryland and the Supreme Court of the United States. This paper was submitted in partial completion of the Master of Laws requirements of the 70th Judge Advocate Officer Graduate Course.

[1] Ellen Nakashima & Paul Sonne, *China Hacked a Navy Contractor and Secured a Trove of Highly Sensitive Data on Submarine Warfare*, WASH. POST, (June 8, 2018; 3:04 PM), https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html.

[2] *See id.* (noting that the contents were not classified, although if aggregated "could be considered classified").

[3] *See id.* (disclosing only basic information concerning the breach without discussing the contractor or the specific purpose of the contractor's work).

[4] *Id.*

[5] *Id.*

undersea combat situation with China."[6] The breach was, unfortunately, not unprecedented. In recent years, as many as 44 percent of defense contractors have been the victim of successful cyber-attacks,[7] many at the hands of China and other adversaries.[8]

These breaches, and the theft of unclassified but sensitive information, are receiving significant attention. The DoD, in order to function, relies upon as many as 300,000 private companies and other entities to supply products and services.[9] These contractors[10] provide crucial support to the DoD's warfighting mission, and in doing so, are often entrusted with sensitive information to perform their requirements.[11] As illustrated above, adversaries have taken advantage of this access and engaged in highly effective, and often high-profile, efforts to obtain information from contractors' cybersecurity systems.[12] Multiple reports detailing widespread deficiencies in contractors' cybersecurity systems,[13] along with the DoD's failure to effectively monitor and identify those deficiencies (despite efforts to do so) have heightened concerns surrounding these attacks.[14]

To more effectively address these concerns, in 2019 the DoD released draft plans to transition to a framework it is calling the Cybersecurity

---

[6] *Id.*

[7] NAT'L DEF. INDUS. ASS'N, BEYOND OBFUSCATION: THE DEFENSE INDUSTRY'S POSITION WITHIN FEDERAL CYBERSECURITY POLICY 21 fig.15 (2019).

[8] *See* Editorial, *Contractors Are Giving Away America's Military Edge*, BLOOMBERG (Apr. 18, 2019, 2:36 PM), https://www.bloomberg.com/opinion/articles/2019-04-18/defense-data-breaches-pentagon-must-hold-contractors-accountable (identifying the actors behind several high-profile breaches of contractor systems).

[9] HEIDI PETERS, CONG. RSCH. SERV., R46643, DEFENSE ACQUISITIONS: DOD'S CYBERSECURITY MATURITY MODEL CERTIFICATION FRAMEWORK 1 (2020).

[10] The term "contractor," as used throughout this article, references "[a]ny individual, firm, corporation, partnership, association, or other legal non-Federal entity that enters into a contract directly with the D[o]D to furnish services, supplies, or construction." 32 C.F.R. § 158.3 (2021).

[11] *See* INSPECTOR GEN., U.S. DEP'T OF DEF., NO. DODIG-2019-105, AUDIT OF PROTECTION OF DOD CONTROLLED UNCLASSIFIED INFORMATION ON CONTRACTOR-OWNED NETWORKS AND SYSTEMS 3 (23 July 2019) [hereinafter DOD IG ROI-CONTRACTOR-OWNED NETWORKS] (discussing the requirements for those contractors who are entrusted with controlled unclassified information).

[12] *See Contractors Are Giving Away America's Military Edge*, *supra* note 8 (describing several high-profile breaches of contractor systems).

[13] *See, e.g.*, DOD IG ROI- CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 7 tbl.2 (identifying significant cybersecurity deficiencies by every contractor evaluated).

[14] *See, e.g.*, DOD IG ROI- CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 27-33 (noting that "[n]either DoD [c]omponent [c]ontracting [o]ffices [n]or DoD [r]equiring [a]ctivities [a]ssessed [c]ontractors' [a]ctions for [p]rotecting [i]nformation" despite requirements to do so).

Maturity Model Certification (CMMC).[15] Since then, the DoD has further refined its model with the release of the CMMC 1.0 framework,[16] an interim rule amending the Defense Federal Acquisition Regulation Supplement (DFARS),[17] and finally, the release of plans for the most current version of the CMMC framework, CMMC 2.0.[18] Under the updated version of the framework, the majority of contractors will self-certify that they have met cybersecurity requirements designed to keep their information systems secure,[19] which continues the DoD's reliance on contractors to review their own cybersecurity measures despite historical challenges associated with this approach.[20]

While the CMMC program is necessary to address glaring weaknesses in contractor cybersecurity,[21] the plan to require such a large group of contractors to self-certify, without significant steps to break from past self-monitoring requirements, is unlikely to meaningfully improve contractors' cyber hygiene.[22] Fortunately, the DoD can supplement the CMMC 2.0 rollout to assure the program overcomes challenges that have stalled past efforts to compel contractors to monitor their own cybersecurity.

First, the DoD should adopt contractual language that clarifies its authority to evaluate contractor cybersecurity systems throughout contract administration.[23] The DoD should also adopt a related clarification of its remedies when a contractor fails to comply with cybersecurity

---

[15] *See* Assessing Contractor Implementation of Cybersecurity Requirements, 85 Fed. Reg. 61505, 61516 (proposed Sept. 29, 2020) (to be codified at 48 C.F.R. § 204) (describing feedback received in response to draft versions of the CMMC model).

[16] *See* Abigail Stokes & Marcus Childress, *The Cybersecurity Maturity Model Certification Explained: What Defense Contractors Need to Know*, CSO, (Apr. 8, 2020, 3:00 AM), https://www.csoonline.com/article/3535797/the-cybersecurity-maturity-model-certification-explained-what-defense-contractors-need-to-know.html (detailing the release of CMMC version 1.0 on 31 January 2020).

[17] Assessing Contractor Implementation of Cybersecurity Requirements, 85 Fed. Reg. 61505 (proposed Sept. 29, 2020) (to be codified at 48 C.F.R. § 204).

[18] *Strategic Direction for Cybersecurity Maturity Model Certification (CMMC) Program* U.S. DEP'T OF DEF. (Nov. 4, 2021), https://www.defense.gov/News/Releases/Release/Article/2833006/strategic-direction-for-cybersecurity-maturity-model-certification-cmmc-program [hereinafter *CMMC Strategic Direction*].

[19] *See* Cybersecurity Maturity Model Certification (CMMC) 2.0 Updates and Way Forward, 86 Fed. Reg. 64100 (Nov. 17, 2021) (providing an overview of certification requirements under CMMC 2.0).

[20] *See, e.g.*, DOD IG ROI-CONTRACTOR-OWNED NETWORKS, *supra* note 11, at i-ii (describing contractors' failures to "consistently implement DoD-mandated system security controls").

[21] *See infra* Part II.A.

[22] *See infra* Part III.

[23] *See infra* Part IV.A.

requirements.[24] This will allow the DoD to discover and act when contractors have failed to properly certify their cyber compliance, while simultaneously acting as a new source of motivation for contractors to comply and accurately evaluate their own systems.[25] To ensure these efforts have a worthwhile impact, however, the DoD will need to utilize existing resources to give component contracting offices the necessary expertise to conduct meaningful inspections.[26] Finally, the DoD should begin to record the data it has gathered on contractor cybersecurity compliance in a consequential manner.[27] These steps, if executed carefully, will greatly increase the chances that this program succeeds where past efforts have failed, and can help ensure an industrial base prepared to counter our adversaries' attempts to obtain sensitive unclassified information.

Part II of this article provides an overview of the history of contractor cyber networks and systems, the circumstances leading up to the CMMC, and the current state of the CMMC framework. Part III then discusses the risks associated with the current path forward, particularly those associated with relying on contractors to self-certify their cybersecurity systems. Finally, Part IV offers a path to address those risks and recommends implementing guidance.

II. Background

A. Vulnerabilities in Contractor Networks and Systems

While security concerns over information in the hands of contractors have been longstanding,[28] over the last decade those concerns have increasingly focused on the cybersecurity precautions contractors have, or have not, taken.[29] A large catalyst behind this shift has been a series of high-profile breaches of contractor systems by adversaries.[30] High-profile

---

[24] *See infra* Part IV.B.
[25] *See infra* Part IV.
[26] *See infra* Part IV.C.
[27] *See infra* Part IV.D.
[28] *See, e.g.*, U.S. GOV'T ACCOUNTABILITY OFF., GAO-03-1037T, INFORMATION SECURITY: FURTHER EFFORTS NEEDED TO FULLY IMPLEMENT STATUTORY REQUIREMENTS IN DOD 29 (2003) (identifying the security of contractor-provided services as a major point of concern).
[29] *See, e.g.*, DOD IG ROI-CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 7 tbl.2 (identifying widespread cybersecurity deficiencies by contractors).
[30] *See Contractors are Giving Away America's Military Edge*, *supra* note 8 (noting the influence of high-profile breaches in describing the need for change).

breaches have included not only the theft of "sensitive data related to naval warfare from the computers of a Navy contractor,"[31] as discussed above, but also the theft of "travel records compromising the personal information and credit card data of U.S. military and civilian personnel"[32] and the theft of F-35 design data,[33] among others.

While these events illustrate individual failures, both internal DoD reviews and Government Accountability Office (GAO) reports have revealed widespread, systemic cybersecurity failures by contractors. The GAO has warned that contractor cybersecurity systems have exposed controlled DoD information, noting in a 2014 report that multiple major agencies, including the DoD, had "reliability issues" just determining which systems were contractor operated.[34] In exploring why these issues were so widespread, the GAO reached the conclusion that "[i]n the past, consideration of cybersecurity . . . was not a focus of key acquisition and requirements policies nor was it a focus of key documents that inform decision-making,"[35] before further noting these failures put weapons systems at risk.[36] Most recently, the GAO indicated that contracting for cybersecurity requirements remains a challenge: "guidance usually did not specifically address how acquisition programs should include cybersecurity requirements . . . and verification processes in contracts."[37]

As early as 2011, the DoD Inspector General found that these issues resulted in serious failures in information security practices by contractors, issuing a report titled "DoD Cannot Ensure Contractors Protected

---

[31] Helene Cooper, *Chinese Hackers Steal Naval Warfare Information*, N.Y. TIMES, (Jun. 8, 2018), https://www.nytimes.com/2018/06/08/us/politics/china-hack-navy-contractor-.html.

[32] Lolita C. Baldor, *Pentagon Reveals Cyber Breach of Travel Records*, ASSOCIATED PRESS (Oct. 12, 2018), https://apnews.com/article/7f6f4db35b0041bdbc5467848225e67d.

[33] David Alexander, *Theft of F-35 Design Data is Helping U.S. Adversaries – Pentagon*, REUTERS (June 19, 2013, 2:36 PM), https://www.reuters.com/article/usa-fighter-hacking/theft-of-f-35-design-data-is-helping-u-s-adversaries-pentagon-idUSL2N0EV0T320130619.

[34] U.S. GOV'T ACCOUNTABILITY OFF., GAO-14-612, INFORMATION SECURITY: AGENCIES NEED TO IMPROVE OVERSIGHT OF CONTRACTOR CONTROLS 22-23 (2014).

[35] U.S. GOV'T ACCOUNTABILITY OFF., GAO-19-128, WEAPON SYSTEMS CYBERSECURITY: DOD JUST BEGINNING TO GRAPPLE WITH SCALE OF VULNERABILITIES 17 (2018) [hereinafter GAO ROI-VULNERABILITIES].

[36] *See id.* at 18 (noting that a lack of focus on cybersecurity puts systems and their related missions at risk).

[37] U.S. GOV'T ACCOUNTABILITY OFF., GAO-21-288, HIGH-RISK SERIES: FEDERAL GOVERNMENT NEEDS TO URGENTLY PURSUE CRITICAL ACTIONS TO ADDRESS MAJOR CYBERSECURITY CHALLENGES 53 (2021).

Controlled Unclassified Information for Weapon Systems Contracts."[38] While the cybersecurity of contractor systems has been the subject of DoD Inspector General reports since then,[39] by late 2016, contractor systems were listed as one of the most frequently reported cybersecurity weaknesses challenging the DoD.[40] A 2019 report titled "Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems" found that every single contractor evaluated in the DoD Inspector General's sample group had significant failures in establishing basic cybersecurity controls.[41] A 2020 report confirmed that risks related to "contractors and third-party partners" remained ongoing, without significant progress, due to failures to implement necessary cybersecurity measures or controls.[42] These cybersecurity shortcomings pose risks to both national security and personal data that need to be addressed hastily.

B. Unsuccessful Legislative and Regulatory Efforts to Address Challenges

Unfortunately, while these challenges have received significant attention, legislative and regulatory efforts to address them have fallen short. Despite substantial requirements to clean up contractor cybersecurity systems, the DoD's consistent failure to provide means of

---

[38] INSPECTOR GEN., U.S. DEP'T OF DEF., NO. DODIG-2011-115, DOD CANNOT ENSURE CONTRACTORS PROTECTED CONTROLLED UNCLASSIFIED INFORMATION FOR WEAPON SYSTEMS CONTRACTS (30 Sept. 2011).

[39] *See, e.g.*, INSPECTOR GEN., U.S. DEP'T OF DEF., NO. DODIG-2015-180, DOD CYBERSECURITY WEAKNESSES AS REPORTED IN AUDIT REPORTS ISSUED FROM AUGUST 1, 2014, THROUGH JULY 31, 2015, at 6-7 (Sept. 25, 2015) (identifying the U.S. Army's continued reliance on voluntary cyber reporting by contractors despite a required DFARS clause language necessitating mandatory reporting as a point of failure).

[40] INSPECTOR GEN., U.S. DEP'T OF DEF., NO. DODIG-2017-034, DOD CYBERSECURITY WEAKNESSES AS REPORTED IN AUDIT REPORTS ISSUED FROM AUGUST 1, 2015, THROUGH JULY 31, 2016, at 5 (14 Dec. 2016). The report was blunt, specifically stating, "[W]e found that the cyber weaknesses most frequently cited . . . [include] contractor systems . . . ." *Id.*

[41] *See* DOD IG ROI-CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 7 tbl.2 (summarizing the flaws identified in each contractor's cybersecurity practices).

[42] *See* INSPECTOR GEN., U.S. DEP'T OF DEF., NO. DODIG-2020-089, SUMMARY OF REPORTS AND TESTIMONIES REGARDING DEPARTMENT OF DEFENSE CYBERSECURITY FROM JULY 1, 2018, THROUGH JUNE 30, 2019, at 12 (11 June 2020) [hereinafter DOD IG REPORTS SUMMARY] (concluding that "significant cybersecurity risks identified in the 46 reports issued and 3 testimonies provided to Congress relate to vendor risk management [and others] . . . . Without adequate controls in those areas, the DoD cannot ensure that . . . contractors and third-party partners implement necessary cybersecurity measures or controls . . . . ").

verification or enforcement have plagued its efforts to improve compliance.

Prior to the CMMC framework, efforts to ensure contractors safeguarded their information systems primarily relied upon mandated breach reporting, threat information sharing, and contractual terms.[43] The first two of these, mandated breach reporting and information sharing, have been helpful but, by their nature, could not ensure satisfactory cyber hygiene. Breach reporting requirements, mandated through the 2013, 2015, and 2019 National Defense Authorization Acts,[44] were not meant to ensure contractors maintained any specific cybersecurity measures. Instead, they were created to ensure awareness of "successful cyber intrusions . . . into the computer networks of operationally critical contractors so that . . . potentially affected combatant commands can assess the risks to contingency operations posed by those intrusions and adjust operational plans, if necessary."[45] Similarly, the DoD's most prominent threat-sharing program for contractors, the Defense Industrial Base Cybersecurity Program, does not require contractors to enact cybersecurity measures or enforce standards.[46] Rather, the voluntary program is simply designed to share information for use in countering threats without prescribing a method or course of action to do so.[47]

Contract terms, on the other hand, have required contractors to meet specific cybersecurity precautions, but have had mixed success. Since 2013, the DoD has used mandatory clauses in the DFARS to require

---

[43] Although these three tools made up the bulk of existing legislative and regulatory mechanisms for encouraging contractor cybersecurity pre-CMMC, it should be noted that these have existed for a relatively short period of time themselves. For a deeper history of cybersecurity requirements as they applied to acquisitions prior to the introduction of these tools see Kui Zeng, Exploring Cybersecurity Requirements in the Defense Acquisition Process (Apr. 23, 2016) (D.Sc. dissertation, Capitol Technology University), (ProQuest).

[44] *See* 10 U.S.C. § 393 (requiring "[r]eporting on penetrations of networks and information systems of certain contractors," and originally enacted by Section 941 of the National Defense Authorization Act for 2013, Pub. L. No. 112-239, 126 Stat. 1632 (2013); *see also* 10 U.S.C. § 391 (requiring "[r]eporting on cyber incidents with respect to networks and information systems of operationally critical contractors and certain other contractors," and originally enacted by section 1632 of the Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291, 128 Stat. 3292 (2014)); 10 U.S.C. § 2224 note (instituting "[r]eporting [r]equirements for [c]ross [d]omain [i]ncidents and [e]xemptions to [p]olicies for [i]nformation [t]echnology," and originally enacted by section 1639 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, 132 Stat. 1636 (2018)).

[45] S. REP. NO. 113-176, at 229 (2014).

[46] *See* 32 C.F.R. § 236.1 (2023) (describing the purpose of the Defense Industrial Base Cybersecurity program).

[47] *See* 32 C.F.R. § 236.6 (2023) (detailing the general provisions of the DoD's Defense Industrial Base Cybersecurity program).

contractors and subcontractors to "provide adequate security on all covered contractor information systems."[48] "Adequate security" is defined as "protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information."[49] More specifically, the DFARS mandates that "the covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, 'Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.'"[50] Since 2016, the Federal Acquisition Regulation (FAR) section 52.204-21 has also imposed additional obligations on non-DoD contractors with the intent to improve cybersecurity practices, which complement the DFARS clauses and NIST SP 800-171.[51] The DFARS clause incorporating NIST SP 800-171 is generally required on all contracts (with limited exceptions),[52] while the clause at FAR 52.204-21 is required on contracts where the contractor or any subcontractor "may have Federal contract information residing in or transiting through its information system" (again with limited exceptions).[53] Both the FAR and DFARS requirements must be passed on to subcontractors by the contractor if the covered sensitive unclassified information will be handled by the subcontractor.[54]

Taken together, these requirements were meant to provide sufficient, if minimum, cybersecurity requirements for contractors to meet their contractual obligations and keep sensitive unclassified information secure. These resources contain the most direct guidance available to contractors in establishing adequate systems. The NIST SP 800-171 provides a series

---

[48] DFARS 204.7302(a)(1) (2022).
[49] DFARS 204.7301 (2022).
[50] DFARS 252.204-7012 (2022).
[51] *See* FAR 52.204-21 (2022) (establishing fifteen minimum requirements for the safeguarding of covered contractor information systems). The language of this clause is required generally by FAR 4.1903 (2022), and in solicitations and contracts for the acquisition of commercial products or commercial services, other than commercially available off-the-shelf items by FAR 12.301(d)(5) (2022).
[52] *See* DFARS 204.7304 (2022) (establishing guidelines for the inclusion of covered defense information clauses).
[53] *See* FAR 4.1903 (2022) (establishing when the insertion of the clause at 48 C.F.R. § 52.204-21 is required).
[54] *See* FAR 52.204-21(c) (2022) ("The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts . . . in which the subcontractor may have Federal contract information residing in or transiting through its information system."). *See also* DFARS 252.204-7012(m) (2022) ("The Contractor shall . . . [i]nclude this clause . . . in subcontracts . . . for operationally critical support, or for which subcontract performance will involve covered defense information . . . . The Contractor shall determine if the information required for subcontractor performance retains its identity as covered defense information and will require protection under this clause . . . .").

of obligations, all of which fall within fourteen "families" of cybersecurity requirements: (1) access control; (2) awareness and training; (3) audit and accountability; (4) configuration management; (5) identification and authentication; (6) incident response; (7) maintenance; (8) media protection; (9) personnel security; (10) physical protection; (11) risk assessment; (12) security assessment; (13) system and communications protection; and (14) system and information integrity.[55] Similarly, FAR 52.204-21 provides fifteen minimum requirements which, for the most part, mirror requirements contained within the NIST SP 800-171 families.[56]

Despite the premise that these requirements should result in sufficiently protected contractor cybersecurity systems, contractor cybersecurity practices have continued to fall short of expectations. Internal reviews and a number of high-profile incidents since the implementation of both the DFARS and FAR requirements make that clear.[57] While there are likely a multitude of reasons for each specific failure, the systemic issues have largely been attributed to the lack of effective verification and enforcement of their terms.[58]

Verification and enforcement have remained a challenge for several reasons. Perhaps most importantly, "neither the FAR clause, nor the DFARS clause, provide for DoD verification of a contractor's implementation of basic safeguarding requirements or the security requirements specified in NIST SP 800-171."[59] The lack of a broad verification program left it up to contracting offices to ensure compliance

---

[55] RON ROSS ET AL., NAT'L INST. OF STANDARDS AND TECH., SP 800-171 REV. 2: PROTECTING CONTROLLED UNCLASSIFIED INFORMATION IN NONFEDERAL SYSTEMS AND ORGANIZATIONS 9-40 (2021).

[56] *See* FAR 52.204-21(b) (2022). *Compare, e.g.*, FAR 52.204-21(b)(1)(iii) (2021) (requiring contractors to "[v]erify and control/limit connections to and use of external information systems") *with* NAT'L INST. OF STANDARDS & TECH., *supra* note 55, para. 3.1.2 (requiring contractors to "[v]erify and control/limit connections to and use of external systems").

[57] *See, e.g.*, DOD IG ROI- CONTRACTOR-OWNED NETWORKS, *supra* note 11, at i-ii (finding that all the contractors audited in the sample group evaluated "did not consistently implement DoD-mandated system security controls for safeguarding Defense information"). *See also Contractors are Giving Away America's Military Edge*, *supra* note 8 (detailing numerous high-profile breaches of contractor systems that occurred after the introduction of NIST SP 800-171 requirements).

[58] *See* U.S. DEP'T OF DEF., DFARS CASE 2019-D041: ASSESSING CONTRACTOR IMPLEMENTATION OF CYBERSECURITY REQUIREMENTS REGULATORY IMPACT ANALYSIS 4 (2020) [hereinafter CYBERSECURITY REQUIREMENTS RIA] (discussing the impact of a lack of verification mechanisms in the cybersecurity contract clauses of the FAR and DFARS).

[59] *Id.*

in awarding and administering contracts,[60] despite the fact that those contracting offices entrusted with monitoring or verification often had no background in the subject.[61] Even when cybersecurity issues were brought to a contracting office's attention, many were still unable to verify compliance or enforce standards because they either felt incapable of acting without higher-headquarters or DoD guidance,[62] did not feel they had "the resources to review compliance,"[63] or did not feel they had the contractual authority to audit contractor systems.[64] As a result, "contracting offices and requiring activities did not implement processes to verify that contractors complied with Federal and DoD requirements for protecting [controlled unclassified information] maintained in non-Federal systems and organizations."[65] This was compounded by the fact that contracting offices did not prioritize cybersecurity and the protection of sensitive unclassified information when evaluating whether to award a contract (or when monitoring a contract during its administration) if they were not the primary focus of a contract's subject matter.[66] Without

---

[60] *See* DOD IG ROI-CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 5-6 (reviewing the responsibility of contracting offices to establish procedures for verifying compliance with cybersecurity contractual requirements, and the failure of those offices to do so). The Defense Counterintelligence and Security Agency (DCSA), by the 17 May 2018 designation of the Office of the Under Secretary of Defense for Intelligence, was tapped to take over many of these responsibilities "as the lead agency for providing oversight of Controlled Unclassified Information (CUI) maintained by DoD contractors." *Id.* at 3. Those responsibilities were enhanced by the publication of DoD Instruction 5200.48, which provided further guidance concerning CUI. U.S. DEP'T OF DEF., INSTR. 5200.48, CONTROLLED UNCLASSIFIED INFORMATION (CUI) (2020). However, DCSA indicates that it is "not currently conducting any oversight of CUI associated with . . . cleared contractors at this time." *Controlled Unclassified Information*, U.S. DEF. COUNTERINTEL. & SEC. AGENCY, https://www.dcsa.mil/mc/ctp/cui (last visited Feb. 7, 2023).

[61] *See*, *e.g.*, DOD IG ROI- CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 28 (detailing how a contracting officer representative tasked with monitoring a contract was unaware of the relevant clauses and path towards NIST SP 800-171 compliance).

[62] *See*, *e.g.*, DOD IG ROI-CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 28 (describing how "[a] Defense Contract Management Agency official . . . stated that the agency was waiting for DoD guidance to establish an assessment process to verify contractor compliance" as the reason the agency had not conducted oversight activities).

[63] DOD IG ROI-CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 28.

[64] *See* DOD IG ROI-CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 28 (summarizing how multiple agencies reported their position did not have contractual authority to audit contractor systems to ensure compliance with contractual requirements and NIST SP 800-171).

[65] DOD IG ROI- CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 4.

[66] *See* DOD IG ROI-CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 32 (revealing that DoD contracting offices often "did not always know which contracts required contractors to maintain [controlled unclassified information] . . . . [and] the DoD does not have a

verification and enforcement, contractors' protection of sensitive unclassified information has not improved.[67]

C. Introduction of the CMMC Framework

As a result of these persistent challenges, the DoD overhauled its approach to contractor cybersecurity by introducing the CMMC framework, which expanded cybersecurity requirements and sought to tackle verification shortcomings.

The initial version of CMMC built upon NIST SP 800-171 and modified the applicable cybersecurity requirements for contractors.[68] The initial framework included tiered standards of cybersecurity, with five CMMC certification levels based on the information the contractor would handle under the contract.[69] While level one certifications essentially required the same security measures as FAR section 52.204-21, security standards increased at each tier under the framework.[70] For example, certification level three, which was standard for contracts handling any controlled unclassified information (CUI), required all of the security levels prescribed in NIST SP 800-171 through DFARS clause 252.204-7012, along with twenty additional practices and three processes.[71]

Beyond this reorganization of security requirements, the original CMMC framework's most novel advancement was the introduction of a verification process for contractors' security practices. It required that, prior to contract award, all contractors pass an assessment at the appropriate CMMC level within the last three years and maintain a current (completed within the last three years) CMMC certification for the duration of the contract.[72] "Third Party Assessment Organizations," or "C3PAOs," conducted the assessments, not the DoD.[73] The process was

process in place to track which contractors maintain [controlled unclassified information]"). *See also* GAO ROI-VULNERABILITIES, *supra* note 35, at 17 (reporting "consideration of cybersecurity was not a focus of the key processes" relating to the acquisition of weapon systems).

[67] *See* DOD IG REPORTS SUMMARY, *supra* note 42, at 12 (noting the continuing failure to make progress in ensuring contractors implement necessary cybersecurity measures).

[68] *See* CYBERSECURITY REQUIREMENTS RIA, *supra* note 58, at 12 (describing the CMMC framework).

[69] CYBERSECURITY REQUIREMENTS RIA, *supra* note 58, at 12.

[70] CYBERSECURITY REQUIREMENTS RIA, *supra* note 58, at 12-13.

[71] CYBERSECURITY REQUIREMENTS RIA, *supra* note 58, at 13.

[72] DFARS 252.204-7021(b) (2022).

[73] *See* CYBERSECURITY REQUIREMENTS RIA, *supra* note 58, at 12 (describing the CMMC contractor assessment process).

market-based; the contractor seeking certification would pay the assessment costs,[74] while C3PAO would pay their own the accreditation costs.[75]

Importantly, these verification requirements would have "flowed down to subcontractors at all tiers," with prime contractors no longer at liberty to distinguish which subcontractors were required to meet cybersecurity standards.[76] Section 252.204-7021 of DFARS was set to begin applying this original CMMC framework to select contracts in fiscal year 2021,[77] with a slow buildup before applying "to all business entities that are awarded a DoD contract" after 1 October 2025.[78]

While this framework seemed poised to aggressively combat the verification and enforcement issues that plagued the contract-based cybersecurity requirements, the program, for a variety of reasons, encountered significant headwinds.[79] In particular, the need to pay for certification was expected to pose substantial costs on small businesses,[80] potentially limiting the DoD's market.[81] There were also very real

---

[74] *See* CYBERSECURITY REQUIREMENTS RIA, *supra* note 58, at 15 (indicating that the "cost of these CMMC assessments will be driven by multiple factors including market forces, the size and complexity of the network or enclaves under assessment, and the CMMC level"). There was initially some indication that these costs would be considered an "allowable cost," which could be reimbursed by the DoD. *See*, *e.g.*, *CMMC Preparation Is An "Allowable Cost" And Reimbursable by DoD*, SYSARC (Aug. 6, 2019), https://www.sysarc.com/cyber-security/cmmc-preparation-is-an-allowable-cost-and-reimbursable-by-dod. However, there is considerable debate that this would be possible, and the DoD has recently removed all previous references to reimbursement from its CMMC material. *See CMMC FAQs*, CHIEF INFO. OFFICER: U.S. DEP'T OF DEF., https://dodcio.defense.gov/CMMC/FAQ/#AboutCMMC (last visited Feb. 7, 2023).

[75] *See* Sara Friedman*, CMMC Accreditation Body Clarifies Details of Approval Process for Assessment Organizations*, INSIDE DEF., (Sept. 2, 2021), https://www.insidedefense.com/share/212555 (stating the requirements for C3PAO assessor certification).

[76] CYBERSECURITY REQUIREMENTS RIA, *supra* note 58, at 16.

[77] CYBERSECURITY REQUIREMENTS RIA, *supra* note 58, at 12. *See also* Letter from Info. Tech. Indus. Council, et al., to Honorable Kathleen Hicks, Deputy Sec'y of Def. (Sept. 8, 2021), https://www.itic.org/documents/public-sector/MultiassociationLetter_CybersecurityPolicy_September2021.pdf.

[78] CYBERSECURITY REQUIREMENTS RIA, *supra* note 58, at 16.

[79] *See CMMC FAQs*, *supra* note 74 (discussing why the DoD transitioned from CMMC 1.0 to CMMC 2.0).

[80] *See* Jackson Barnett, *Department of Defense to Address Small Business Concerns as Part of CMMC Program Review*, FEDSCOOP (June 28, 2021), https://www.fedscoop.com/department-of-defense-to-address-small-business-concerns-as-part-of-cmmc-program-review (detailing concerns with the cost of CMMC certification for small businesses).

[81] *See, e.g.*, *CMMC Implementation: What It Means for Small Businesses: Hearing Before the H. Small Bus. Subcomm. on Oversight, Investigations & Regul. of the H. Small Bus. Comm.,* 117th Cong. (2021) (statement of Michael Dunbar, President, Ryzhka International).

concerns that the plan to independently certify the approximately 300,000 DoD contractors was simply not feasible.[82] These concerns increased when the number of assessors fell far short of initial estimates.[83]

In response to these issues, the DoD drastically changed its CMMC implementation plan in November of 2021 when it released initial plans for "CMMC 2.0."[84] While specifics regarding the new framework remain in development, some changes are clear. First, the standards more closely align with NIST standards, eliminating maturity processes and security practices unique to the CMMC.[85] Second, the DoD removed levels two and four from the five CMMC certification levels, which were transitional and allowed contractors to smoothly move between levels one, three, and five.[86] Under the new system, contractors who handle "Federal Contract Information"[87] (FCI) will require a level-one certification, those who handle any CUI[88] will require a level-two certification, and those contractors facing a particularized risk from "Advanced Persistent Threats" will be required to obtain a level-three certification.[89] Most importantly for our purposes, the third-party assessment framework was

---

[82] *See,* Federal Drive with Tom Temin, *DoD's Plan for Contractor Cybersecurity Lacks a Few Things, Money's Only One of Them*, FED. NEWS NETWORK (June 18, 2021, 12:55 PM), https://federalnewsnetwork.com/cybersecurity/2021/06/dods-plan-for-contractor-cybersecurity-lacks-a-few-things-moneys-only-one-of-them.

[83] *Id.*

[84] *See CMMC Strategic Direction*, *supra* note 18 (announcing the launch of CMMC 2.0 and describing changes from CMMC 1.0 in broad terms).

[85] Cybersecurity Maturity Model Certification (CMMC) 2.0 Updates and Way Forward, 86 Fed. Reg. 64100 (Nov. 17, 2021).

[86] *Id.*

[87] "Federal Contract Information" is defined within the CMMC framework as "information provided by or generated for the Government under contract not intended for public release." CARNEGIE MELLON UNIV. & THE JOHNS HOPKINS UNIV. APPLIED PHYSICS LAB'Y, Cybersecurity Maturity Model Certification (CMMC) Model Overview 1 (2021), https://dodcio.defense.gov/Portals/0/Documents/CMMC/ModelOverview_V2.0_FINAL2_20211202_508.pdf (citing 48 C.F.R. § 252.204-21 (2016)).

[88] "Controlled Unclassified Information" is defined within the CMMC framework as "information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations, and government-wide policies, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or Atomic Energy Act of 1954, as amended." CARNEGIE MELLON UNIV. & THE JOHNS HOPKINS UNIV. APPLIED PHYSICS LAB'Y, *supra* note 87, at 1 (citing NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COM., SP 800-171, PROTECTING CONTROLLED UNCLASSIFIED INFORMATION IN NONFEDERAL SYSTEMS AND ORGANIZATIONS 9-40 (2nd rev. 2021)).

[89] *See* CARNEGIE MELLON UNIV. & THE JOHNS HOPKINS UNIV. APPLIED PHYSICS LAB'Y, *supra* note 87, at 16 (summarizing the criteria for each level of certification under the CMMC).

removed for both level-one contractors,[90] who constitute the vast majority of DoD contractors,[91] and those level-two contractors involved with "non-prioritized acquisitions," which is estimated to be approximately half of the contractors handling CUI.[92] The third-party assessment for both of these groups has instead been replaced by an annual self-assessment.[93]

The return to a self-assessment framework once again puts the majority of contractors in a position to self-certify compliance with relevant cybersecurity requirements. While the pivot to CMMC 2.0 provided necessary relief to what would have been a significantly overburdened assessment system and a scrambling industrial base, self-assessments bring back the same set of challenges the DoD wrestled with in its past efforts to ensure effective cybersecurity. Third-party assessors brought accountability[94] to a population that often failed to uphold its cybersecurity responsibilities when allowed to self-monitor.[95] The return to contractor-led compliance, on the other hand, maintains the status quo despite its lack of success.

---

[90] Cybersecurity Maturity Model Certification (CMMC) 2.0 Updates and Way Forward, 86 Fed. Reg. 64100 (Nov. 17, 2021) (providing an overview of certification requirements under CMMC 2.0).

[91] *See* Jason Doubleday, *Pentagon Strips Down CMMC Program to Streamline Industry Cyber Assessments*, FED. NEWS NETWORK (Nov. 4, 2021, 2:09 PM), https://www.federalnewsnetwork.com/defense-main/2021/11/pentagon-strips-down-cmmc-program-to-streamline-industry-cyber-assessments.

[92] *See* Cybersecurity Maturity Model Certification (CMMC) 2.0 Updates and Way Forward, 86 Fed. Reg. at 64100. There has been some indication that this may change in the future, and all level-two contractors will be required to obtain a third-party CMMC assessment. *See* Jason Doubleday, *More Companies May Have to Get a CMMC Assessment After All*, FED. NEWS NETWORK (Feb. 10, 2022, 6:42 PM), https://www.federalnewsnetwork.com/cybersecurity/2022/02/more-companies-may-have-to-get-a-cmmc-assessment-after-all. However, the official position of the DoD remains that only a portion of companies handling CUI will be required to obtain a third-party assessment. *See CMMC FAQs*, *supra* note 74 (indicating that only "some" level-two contractors will be required to obtain a third-party assessment).

[93] *See* Cybersecurity Maturity Model Certification (CMMC) 2.0 Updates and Way Forward, 86 Fed. Reg. at 64100 (providing an overview of requirements under CMMC 2.0).

[94] *See* Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041), 85 Fed. Reg. 61505 (proposed Sept. 29, 2020) (to be codified at 48 C.F.R. § 204) (outlining third party accessor requirements of CMMC 1.0).

[95] *See* discussion *supra* Part II.B (summarizing contractor cybersecurity challenges).

III. Challenges to Effective Certification Under the New Self-Evaluation Framework

The ongoing reliance on self-evaluations, without outside review, is a real issue that impacts national security; weak systems that provide an avenue for adversaries to access FCI and CUI have repeatedly enabled them to counter our abilities and expand their own.[96] The status quo must change. Self-evaluation as a primary means of accountability for DoD contractors is a tried and failed approach.[97] Mandatory FAR and DFARS provisions have required DoD contractors to meet cybersecurity standards for years.[98] Contractors, however, were left to self-monitor their compliance under that framework, and the result has been an almost uniform failure to effectively do so.[99] The recent withdrawal of third-party certification requirements without any substantial substitution to motivate contractor compliance essentially brings requirements full circle.[100] The plan lacks any truly novel means of review or enforcement not present under the previous framework.

Removing third-party assessments also removes a significant source of expertise without an obvious replacement. Many contracting offices lack the expertise to internally verify compliance even if they identify an issue.[101] The third-party assessor program addressed this challenge by providing a host of resources and an assessor who could evaluate efforts, identify weaknesses, and knowledgeably evaluate compliance.[102] With

---

[96] *See, e.g.*, Ellen Nakashima & Paul Sonne, *supra* note 1 (describing the impact of the loss of sensitive, unclassified FCI and CUI to the Chinese Ministry of State Security).

[97] *See* discussion *supra* Part II.B (describing the failures of the contractual clause requirements in establishing effective contractor cyber hygiene).

[98] *See* DFARS 204.73 (2022) (detailing cybersecurity requirements for FCI and CUI). *See also* FAR 52.204-21 (2022) (establishing 15 minimum requirements for the safeguarding of covered contractor information systems).

[99] *See* DOD IG ROI- CONTRACTOR-OWNED NETWORKS, *supra* note 11, at i-ii (finding that all the contractors audited in the sample group evaluated "did not consistently implement DoD-mandated system security controls for safeguarding Defense information"). *See also Contractors are Giving Away America's Military Edge*, *supra* note 8 (detailing numerous high-profile breaches of contractor systems that occurred after the introduction of NIST SP 800-171 requirements).

[100] Self-assessments will be conducted along the same standards that existed prior to CMMC implementation. The only additional requirement is "an annual affirmation by a senior company official." *CMMC Assessments*, CHIEF INFO. OFFICER, U.S. DEP'T OF DEF., https://dodcio.defense.gov/CMMC/Assessments (last visited Feb. 7, 2023) (previewing the assessment process under CMMC 2.0).

[101] *See* DOD IG ROI- CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 28 (describing contracting office's lack of understanding of cybersecurity systems and requirements).

[102] *See* CYBERSECURITY REQUIREMENTS RIA, *supra* note 58, at 13-15 (describing the role of assessors in the CMMC framework).

that program gone, contracting offices are left in some cases to do little more than guess whether contractors have appropriately addressed requirements.

These challenges are significant. Cumulatively, the return to a self-evaluation model, the absence of any new means of enforcement, and the lack of cybersecurity knowledge amongst contracting offices threaten to prevent the CMMC framework from reaching its most important goal: ensuring contractors meet appropriate cybersecurity requirements.[103] The question then becomes: what actions can be taken to address these challenges within the CMMC 2.0 framework in order to ensure that goal is met?

IV. Necessary Steps to Ensure Effective Self-Evaluations

Now, as the DoD is finalizing and preparing rules for CMMC 2.0, is the moment to take action to address the challenges associated with self-evaluations. This can be done by allowing a robust inspection system to flourish. To do so, the DoD should first clarify rights of access to allow contracting offices to effectively monitor contractors' self-evaluations. This can be done by updating mandatory clauses in the DFARS, or, in the interim, through the inclusion of contract-specific clauses.[104] Second, contracting officers' remedies to correct and deter deficiencies must be clarified.[105] Third, contracting offices need to effectively utilize clarified rights of access, and remedies, to effectively audit contractors, identify failures, and motivate others to self-evaluate. As discussed below, using locally appointed government technical monitors can achieve these goals without expending vast resources.[106] Finally, the DoD can, and should, ensure it retains the data from this inspection framework to document contractor past performance and identify systemic difficulties in cybersecurity compliance so that it can better address future challenges.[107]

---

[103] *See About CMMC*, CHIEF INFO. OFFICER, U.S. DEP'T OF DEF., https://www.dodcio.defense.gov/CMMC/About (last visited Feb. 7, 2023) (describing the CMMC program).
[104] *See infra* Part IV.A.
[105] *See infra* Part IV.B.
[106] *See infra* Part IV.C.
[107] *See infra* Part IV.D.

A. Clarifying Contractual Cybersecurity Monitoring Authorities

Without a means of verifying contractor cyber hygiene prior to contract formation, attempts to ensure cybersecurity requirements are fulfilled must shift to the contract management phase. Yet, as discussed above,[108] multiple DoD agencies believe they are essentially powerless during this period, stating that they do "not have the contractual authority to oversee compliance on contractor networks."[109] That must change if any effective means of verification and enforcement are to take place, and it is imperative that clear contractual authority to inspect contractor cybersecurity systems be a part of the modified CMMC framework going forward.

"Inspection . . . is the primary means of ensuring that the government receives that for which it bargained."[110] The FAR, recognizing this importance, requires agencies to "ensure that . . . contracts include inspection . . . requirements . . . [and that] [n]o contract precludes the Government from performing inspection."[111] Similarly, the DFARS recognizes the importance of inspection in ensuring contract requirements are met, requiring "[d]epartments and agencies . . . [to] [a]pply Government quality assurance to all contracts for services and products . . . [and] [c]onduct quality audits to ensure the quality of products and services meet contractual requirements."[112]

All of these requirements emphasize one thing: if a good or service is an important part of contract performance, the contract should provide the Government with a means of inspection.[113] The CMMC framework is, at its core, a push to make adherence to contractual cybersecurity

---

[108] *See supra* Part II.B.

[109] DOD IG ROI-CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 28. There appears to be some debate about whether contractual authority to oversee compliance exists among DoD agencies. *See id.* (discussing the confusion around whether assessing contractor networks and systems is permissible). Inspections that occur but were unforseen by contract can have several negative consequences for the government, including the obligation to cover increased costs to the contractor. *See* JOHN CIBINIC, JR. ET AL., ADMINISTRATION OF GOVERNMENT CONTRACTS 700-06 (5th ed. 2016) (describing the impact of improper inspections). Even if access to contractor networks were eventually found to be permissible under current default contract language by a reviewing authority, the existing confusion even among DoD components means that the current default language presents at the very least the risk of litigation and associated delays.

[110] CIBINIC, JR. ET AL., *supra* note 109, at 698.

[111] FAR 46.102(d) (2022).

[112] DFARS 246.102(1)-(2) (2022).

[113] *See, e.g.*, DFARS 246.102 (2022) (detailing DoD's systemic quality assurance program to ensure contract performance to specified requirements).

requirements a critical component of contract performance.[114] The first step toward aligning these goals is a right of access in all contracts involving sensitive unclassified information so that cyber hygiene can be inspected and evaluated just like other critical components of contract performance.

This can be accomplished in two ways. First, and most immediately, DoD contracting offices can individually insert clear, unambiguous clauses into future contracts that ensure a right to inspect information systems. Right to inspect clauses "would allow representatives of the agencies to assess the cybersecurity protections implemented on contractor networks and systems,"[115] as the DoD Inspector General has advocated regarding contractors maintaining CUI.[116] These clauses could be modeled upon existing language that allows for inspection rights,[117] and would overcome DoD agencies' concern that they do "not have the contractual authority to oversee compliance on contractor networks."[118] With a clear method to evaluate cybersecurity self-assessments enshrined in the contract, contractors are also put on notice that inspections of their cybersecurity systems and self-evaluations are a distinct possibility, increasing motivations to improve compliance.

In the long term, however, clauses prepared for individual contracts on an ad-hoc, local basis carry minor risks. These risks range from the relatively harmless, such as failing to ensure a sufficiently broad right of access to systems,[119] to the more serious risk of failing to provide for the proper type of inspection, potentially preventing a meaningful assessment,[120] or even allowing the contractor to recover costs in the

---

[114] *See About CMMC*, *supra* note 103 (describing the renewed priority of cybersecurity in DoD contracting).

[115] DOD IG ROI-CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 28-29.

[116] *See* DOD IG ROI-CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 28-29 (advocating for the adoption of right-to-audit statements in contracts by DoD component contracting offices).

[117] *See, e.g.,* FAR 52.227-14 (2022) (Alternate V) (allowing the contracting officer the opportunity to "inspect at the Contractor's facility any data withheld" to verify the contractor's assertion of limited rights of data or for evaluating work performance). *See also* FAR 52.246-12 (2022) (inspection of construction clause); FAR 52.246-4 (2022) (inspection of services clause).

[118] DOD IG ROI- CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 28.

[119] *See* CIBINIC, JR. ET AL., *supra* note 109, at 706-07 (discussing the impact of the language used in inspection clauses on the permissible place and time of ensuing inspections).

[120] *See* CIBINIC, JR. ET AL., *supra* note 109, at 701-05 (analyzing the impact of language used in inspection clauses on the types of inspections the government may perform).

future.[121] Standardized, mandatory inspection clauses, paired with the mandatory cybersecurity requirements in DFARS 252.204-7012[122] and FAR 52.204-21,[123] and any additional requirements implemented by CMMC 2.0 can solve these problems.[124] A thoroughly prepared and vetted mandatory right-to-inspect clause can provide for the necessary inspections to evaluate compliance with minimal risk of an oversight that could cause problems later.[125] With the risk minimized, the mandatory clause can guarantee a right of access and put contractors on notice that their self-certifications will be evaluated, just as individually inserted clauses would seek to do in the short term.

Failing to move forward with clear right of access clauses leaves few other measures for the DoD to verify contractors' cybersecurity assertions. Relying on current contract language is, as discussed above, insufficient to ensure DoD can verify compliance at any stage of the contracting process.[126] The DoD could, alternatively, move towards a framework in which verification is outsourced to third parties or conducted prior to contract formation, as opposed to seeking to clarify its own right of access during contract administration. However, these options were contemplated by CMMC 1.0[127] and eventually rejected.[128] There was insufficient third-party interest to support the large number of assessors necessary to support

---

[121] *See, e.g.*, Appeal of Kenyon Magnetics, Inc., 1977 GSBCA LEXIS 103 (Gen. Serv. Admin. B.C.A., Sept. 30, 1977) (in which the contract failed to put the contractor on notice regarding the inspection conducted, and associated delays allowed an equitable adjustment).

[122] DFARS 252.204-7012 (2022).

[123] FAR 52.204-21 (2022).

[124] *See About CMMC*, *supra* note 103 (indicating that the DoD "intends to pursue rulemaking" at both Part 32 and Part 48 of the Code of Federal Regulations in implementing CMMC 2.0).

[125] There is still the risk that the mandatory clause could be inadvertently left out of the contract, of course, but that risk is minimal. Regular, important emphasis on the significance of such a clause could eliminate this minimal risk if it leads to the clause's inclusion in future contracts under the *Christian* doctrine, first enunciated in G.L. Christian & Assocs. v. United States, 312 F.2d 418, 426 (Ct. Cl. 1963). *See* Michael D. Pangia, *The Unpredictable and Often Misunderstood Christian Doctrine of Government Contracts: Proposed Approaches for Removing Harmful Uncertainty*, 49 Pub. Cont. L.J. 617, 629-35 (2020) (providing an overview of current requirements for reading an absent clause into a government contract under the *Christian* doctrine).

[126] *See* discussion *supra* Part III.

[127] *See* CYBERSECURITY REQUIREMENTS RIA, *supra* note 58, at 14-15 (laying out a plan in which all contractors handling FCI and CUI were assessed by third-party evaluators prior to contract performance).

[128] *See About CMMC*, *supra* note 103 (stating that all contractors only handling FCI, and a portion of contractors handling CUI, would not undergo third-party assessments or any other sort of outside assessment prior to contract performance).

such a large number of third-party assessments,[129] and the cost was prohibitive.[130] Similarly, shifting evaluations to the contract formation stage would quickly become overwhelming because the DoD would need to consider evaluating not just successful awardees, but also all competing contractors, increasing its workload many times over. Instead, by ensuring a right of access during contract administration, the DoD maintains the ability to evaluate systems and motivate compliance, but on a manageable scale.

B. Establishing Remedies

With a clearer authority to oversee and inspect cybersecurity on contractor networks, the DoD can address concerns that arise during inspections by creating and clarifying contractual noncompliance remedies. Inspections are generally paired with consequences to motivate compliance[131] because the risk that the benefits of the contract may be lost through noncompliance lies at the core of the overall effectiveness of the inspection framework.[132] The DoD does currently have some tools available should it discover concerns, and continued reliance on these tools represents the primary alternative to instituting new contractual language specifying additional remedies. However, there are significant benefits to inserting language in the DFARS that creates and clarifies contracting offices' remedies for noncompliance, and the DoD could easily include such language in the proposed inspection clause discussed above.

A significant body of research on the interrelations between inspections and compliance "reinforce[s] the importance of inspections for compelling compliance."[133] While the mere possibility that an inspection may occur is often enough to motivate compliance,[134] consequences for

---

[129] *See* Christopher Burgess, *Lack of C3PAO Assessors Jeopardizes DoD CMMC Certification Goal*, CSO (Sept. 8, 2021, 2:00 AM), https://www.csoonline.com/article/3632398/lack-of-c3pao-assessors-jeopardizes-dod-cmmc-certification-goal.html (reporting that only 100 approved assessors had obtained certification despite the need for 5,000 to meet requirements under the original CMMC framework).

[130] *See* Barnett, *supra* note 80 (discussing the financial impact of third-party CMMC assessments on small businesses).

[131] *See* Peter J. May, *Compliance Motivations: Affirmative and Negative Bases*, 38 L. & SOC'Y REV. 41, 45 (2004) (discussing the impact of inspection frequency, thoroughness, and consequences on compliance across a range of studies).

[132] *See id.*

[133] *Id.*

[134] *See id.* (comparing the impact of inspections on compliance with the impact of sanctions resulting from those inspections).

noncompliance are an important additional step, capable of ensuring that those who may not otherwise be inclined to comply are convinced to do so.[135] Consequences not only motivate the deficient contractor, but also deter others by making them aware of the potential costs of non-compliance.[136] This is most effective when the potential consequences are clear, known, and predictable.[137]

Unfortunately, the consequences for noncompliance with DoD cyber requirements have been unclear and unenforced, even when deficiencies are well known.[138] The DoD currently has several options to address contractor performance, which it could continue to rely on exclusively for cybersecurity failures. These include, but are not limited to, breach of contract claims,[139] terminations,[140] and causes of action under the False Claims Act (FCA).[141] However, there are concerns with each of these remedies in the cybersecurity context.

Regarding any breach claims, the biggest impediment is that damages will often be impossible to prove absent a known security breach with an accompanying loss of data.[142] Without known damages, a breach of contract claim carries no substantial penalty.[143] Terminations, likewise,

---

[135] *See id.* at 43 (providing an overview of "[t]he traditional toolkit for obtaining compliance . . . through enforcement actions and imposition of sanctions for those found to be out of compliance").

[136] *See id.* at 42 (discussing the deterrent basis for compliance).

[137] *Id.* Importantly, the severity of these consequences is generally not the most significant factor behind their effectiveness. *See id.* at 46 (noting "mixed" outcomes of studies concerning the effect of the level of sanctions on compliance).

[138] *See* DOD IG ROI- CONTRACTOR-OWNED NETWORKS, *supra* note 11, at iii (describing contracting offices' confusion regarding contractor systems and its impact on correcting performance).

[139] Government claims for breach of contract remain available even when the contract does not provide for a specific relief. *See PAE Int'l.*, ASBCA 45314, 98-1 BCA ¶ 29,347 (indicating that "[o]n the other hand, 'when only partial relief is available under the contract . . . the remedies under the contract are not exclusive and the . . . [party seeking damages] may secure damages in breach of contract'" in finding that the Government could recover damages caused by the contractor's theft of fuel) (quoting United States v. Utah Construction and Mining Co., 384 U.S. 394, 402 (1996)).

[140] For default or convenience. *See, e.g.*, FAR 52.249-2 (2022) (termination for convenience of the government clause for fixed-price contracts).

[141] *See* 31 U.S.C. § 3729 (containing the civil provision of the False Claims Act). *See also* 18 U.S.C. § 287 (containing the criminal provisions of the False Claims Act).

[142] *See PAE Int'l.*, ASBCA 45314, 98-1 BCA ¶ 29,347 (indicating that an "injured party in an action for breach of contract is [only] entitled to recover for two types of loss: 'the loss in the value to him of the other party's performance caused by its failure or deficiency' and 'any other loss, including incidental or consequential loss, caused by the breach . . . .'") (quoting the RESTATEMENT (SECOND) OF CONTRACTS § 347 (AM. L. INST. 1981) (Measure of Damages in General)).

[143] *See id.*

are of limited utility. A termination ends contract performance,[144] which may work in some circumstances, but leaves little room to be a useful tool to encourage compliance if the requiring activity does not have the flexibility to overcome the loss of the contract prematurely.

In cases in which the contractor has falsely certified that their system meets cyber requirements, the FCA is perhaps the most on-point remedy, and is currently one of the recommended tools to address lax contractor cybersecurity.[145] Despite this, there are significant concerns to utilizing the FCA as the main tool to address failures. First, it is not a guaranteed solution. FCA liability can only be imposed when the requirement is "material."[146] Whether cybersecurity requirements will meet the definition of material in most contracts is an open dispute, and at least one reviewing authority has determined that such requirements are not material, at least under certain circumstances.[147]

FCA claims must also show that any noncompliance was done "knowingly."[148] This is also a potential point of failure as it will be difficult for the Government to meet its burden.[149] Even if these concerns were satisfied, however, FCA claims are a drastic remedy in which the DoD loses some control and the Department of Justice becomes the lead agency to pursue serious civil or even criminal consequences.[150]

This is simply not a feasible solution for improving compliance when, under the most recent internal DoD audits, essentially *every contractor* is

---

[144] *See, e.g.*, FAR 52.249-2 (2022).

[145] *See Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative*, U.S. DEP'T OF JUST. (Oct. 6, 2021), https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative (stating that "[t]he Civil Cyber-Fraud Initiative will utilize the False Claims Act to pursue cybersecurity related fraud by government contractors and grant recipients").

[146] "Material" is defined as "having a natural tendency to influence, or be capable of influencing, the payment or receipt of money or property." 31 U.S.C. § 3729(b)(4).

[147] *See* United States *ex rel.* Adams v. Dell Computer Corp., 496 F. Supp. 3d 91 (D.D.C. 2020) (dismissing the *qui tam* suit on the basis that noncompliance with cybersecurity requirements was not material).

[148] "Knowingly" requires that the contractor "(i) has actual knowledge of the information; (ii) acts in deliberate ignorance of the truth or falsity of the information; or (iii) acts in reckless disregard of the truth or falsity of the information." 31 U.S.C. § 3729(b)(1).

[149] *See, e.g.*, Michael Wagner et al., *Cybersecurity and Government Contracting: False Claims Act Considerations*, COVINGTON, (Jan. 11, 2021), https://www.insidegovernment contracts.com/2021/01/cybersecurity-and-government-contracting-false-claims-act-considerations (detailing concerns regarding the requirement to show noncompliance was "knowing" in the context of cybersecurity FCA claims).

[150] *See* 31 U.S.C. § 3729 (containing the civil provision of the False Claims Act). *See also* 18 U.S.C. § 287 (containing the criminal provisions of the False Claims Act).

failing to meet some of their low-level cybersecurity requirements.[151] The DoD does not, and would not, use the FCA in other contexts to address every instance of contractor underperformance, and it should not with cybersecurity. To do so would be inappropriately heavy-handed; relying on sanctions of this nature to address such common issues will likely degrade trust and legitimacy and will harm compliance efforts more than help them.[152]

Instead, the DoD should follow the same playbook it uses to seek corrections for other aspects of performance: contractual remedies included under the applicable inspection clause.[153] Inspection clauses that address other aspects of performance, including services,[154] supplies,[155] or construction,[156] allow the DoD "(1) to require contractor correction, (2) to correct the defects itself or have them corrected by another contractor, charging the contractor for the expense, (3) terminated [sic] for default, or (4) to obtain a price reduction."[157] These standard remedies provide a basic framework for consequences in cases of cybersecurity noncompliance and can be easily applied in this context.[158] Making the DoD's right to demand post-inspection corrections to cybersecurity safeguards explicit can only make obtaining these corrections easier. It can also help avoid any costs the contractor might seek to pass on to the DoD for bringing its systems into compliance.

Prominently stating that terminations are appropriate when cybersecurity requirements are not met boldly demonstrates that these requirements are an essential part of contractor performance. Tailored price adjustment language could allow the DoD to reduce the contract price by the amount of money the contractor saved by not implementing the necessary corrections, as it has done in other contexts.[159]

---

[151] *See* DOD IG ROI-CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 7 tbl.2 (noting that every contractor audited showed significant cybersecurity control deficiencies).
[152] *See* May, *supra* note 131, at 47 (describing the impact of trust and legitimacy on compliance).
[153] *See* CIBINIC, JR. ET AL., *supra* note 110, at 756-61 (detailing the government's remedies for issues identified during inspections under the various inspection clauses of the FAR).
[154] *See, e.g.*, FAR 52.246-4 (2022) (regarding inspection of services-fixed-price).
[155] *See, e.g.*, FAR 52.246-3 (2022) (regarding inspection of supplies-cost-reimbursement).
[156] *See* FAR 52.246-12 (2022) (regarding inspection of construction).
[157] CIBINIC, JR. ET AL., *supra* note 109, at 756.
[158] Remedy (2), charging the contractor for corrections made to their work, is the only remedy likely inapplicable to the cyber context because we are seeking to correct the contractor's own systems. *See* CIBINIC, JR. ET AL., *supra* note 109, at 758-59.
[159] *See, e.g.*, Techni Data Labs., ASBCA 21054, 77-2 BCA ¶ 12,667 (finding the Government was entitled to an equitable adjustment reducing the contract price by $17,514 because the contractor had saved that amount by failing to correct deficiencies in its performance).

By crafting an inspection clause that clearly authorizes these standard government remedies as the situation dictates, the DoD can alleviate essentially all the concerns discussed above with existing means of enforcement. The DoD could compel correction without having to prove damages, resort to termination in every case, or rely on the FCA to address what is a very common issue that rarely requires criminal or civil judicial action.[160] Just as importantly, with remedies specifically spelled out in the contract, both contracting officers and contractors will have clear, known, predictable consequences for non-compliance, which are vital to motivating compliance going forward.

C. Meaningfully Evaluating Contractor Performance

Once the DoD's ability to inspect cybersecurity systems and act to address deficiencies is clearer, the DoD must actually evaluate contractor performance to motivate compliance and uncover systemic challenges. Meaningful evaluations can overcome the obstacles that plagued the prior self-evaluation framework and can lead to a healthier cyber environment throughout the defense industrial base.

While, as discussed above, the Government's clear right to inspect cybersecurity systems motivates compliance, that effect relies upon the possibility that the DoD will, indeed, inspect. Inspections that correctly identify issues will, for the most part, result in corrections.[161] While this sounds straightforward, relying on contracting officers and contracting officer representatives to evaluate cybersecurity requirements as part of their general contract administration duties has failed.[162] Although this was due in part to some agencies' belief that they could not access contractor systems,[163] even where access was not an issue, contracting officers and contracting officer representatives simply lacked the expertise to identify concerns.[164] An alternative attempt to move inspection responsibility outside contracting offices (by requiring what was

---

[160] There will still, however, be a place for FCA action when the facts warrant it.

[161] *See, e.g.*, DOD IG ROI-CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 8-10 (discussing actions taken by contractors once it was discovered, and they were informed, that they had failed to implement required multifactor authentication requirements).

[162] *See* discussion *infra* Part II.B.

[163] *See* DOD IG ROI-CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 28 (discussing some agencies' beliefs that existing contract language did not allow them to review contractor cyber networks).

[164] *See* DOD IG ROI-CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 28 (stating that contracting officers and their representatives did not feel they had "the resources to review compliance").

essentially a mandatory pre-inspection via the CMMC third-party certification framework) also failed after the plan's public comments and feedback steered the DoD in a different direction.[165]

A middle ground between these approaches adds expertise to the contractor cybersecurity evaluations while continuing to rely on the local contracting office that's administering requirements: the appointment of a technical representative with cybersecurity expertise to conduct inspections and advise the contracting officer's representative. This is a need that has already been anticipated in other contexts. For example, the Department of State Acquisition Regulation (DOSAR), which is the Department of State's FAR supplement, already anticipates the need for such an individual. Part 642 of DOSAR, governing contract administration and audit services, states:

> The contracting officer may appoint a Government Technical Monitor (GTM) to assist the Contracting Officer's Representative (COR) in monitoring a contractor's performance. The contracting officer may appoint a GTM because of physical proximity to the contractor's work site, or because of special skills or knowledge necessary for monitoring the contractor's work. The contracting officer may also appoint a GTM to represent the interests of another requirements office or post concerned with the contractor's work. A GTM shall be a direct-hire U.S. Government employee.[166]

An individual with the right knowledge and responsibilities, appointed with or without the DoD's adoption of a similar provision in the DFARS,[167] is perfectly positioned to fill the knowledge gap that has

---

[165] *See About CMMC*, *supra* note 103 (announcing the withdrawal of the CMMC 1.0 framework after receiving "more than 850 public comments in response to the interim DFARS rule").

[166] DOSAR 642.271 (2020). The title "Government Technical Monitor" (GTM), as used here, references a person distinct from the contracting officer's representative. It is not, as used by some agencies in the past, an alternative means of identifying an individual with contracting officer's representative responsibilities. *See, e.g.*, U.S. DEP'T OF HOUS. & URB. DEV., HUD-1044 ASSISTANCE AWARD/AMENDMENT (1990), https://www.hud.gov/sites/documents/1044.PDF (referencing a "Government Technical Representative" in section 9).

[167] While a rule reflecting a policy position in favor of the use of GTMs would be helpful, nothing currently bars contracting officers from appointing individuals with GTM duties. *See* U.S. DEP'T OF DEF., CONTRACTING OFFICER'S REPRESENTATIVES GUIDEBOOK 15 (2021) (noting "these functions and contract surveillance are not solely the responsibility of the Contracting Officer and the COR; other individuals may have designated surveillance responsibilities").

hindered contracting officers and contracting officer representatives in the past. The DoD already employs at least 70,000 cybersecurity professionals,[168] and has a total combined information technology and cyber workforce of at least 150,000 people[169] managing an inventory spread over 5,000 locations.[170] Cybersecurity and/or information technology professionals from the DoD will almost always be located at or near the place of contract performance. These individuals can review the contractors' self-evaluations as long as contracting officers and contracting officer representatives are empowered to collaborate with them.

Utilizing existing cybersecurity and information technology experts is unlikely to impose any excessive burden on Government personnel. Inspections can occur infrequently at the Government's convenience (i.e., when personnel are available, and when inspections will not impact everyday duties), and should never take more than three hours.[171] Moreover, there should not be significant additional cost for the Government to utilize its own employees on a relatively rare basis.[172] Contractors should not face significant expenses either. Any additional costs associated with correcting deficiencies is attributable to meeting

---

[168] *See* C. Todd Lopez, *DOD Mission Big Draw for Cyber Defense Job Applicants*, U.S. DEP'T OF DEF., (Nov. 14, 2019), https://www.defense.gov/News/News-Stories/Article/Article/2017163/dod-mission-big-draw-for-cyber-defense-job-applicants (indicating that the department had 70,000 cyber professionals but intended to hire thousands more going forward).

[169] Jared Serbu, *DoD has a New Plan to Apply Enterprise-Wide Talent Management to its Cyber Workforce*, FED. NEWS NETWORK (Mar. 10, 2023, 7:11 AM), https://www.federalnewsnetwork.com/defense-news/2023/03/dod-has-a-new-plan-to-apply-enterprise-wide-talent-management-to-its-cyber-workforce/.

[170] *See* U.S. DEP'T OF DEF., DOD DIGITAL MODERNIZATION STRATEGY 7 (2019).

[171] Three hours is the estimated amount of time DoD assessors will need to conduct mid-tier level contractor assessments under the NIST SP 800-171 DoD Assessment Methodology, which was originally rolled out at the same time as CMMC 1.0. Inspections are not meant to replace assessments and should not be more in depth or take more time than standardized DoD assessments evaluating contractors who handle more sensitive information than those contractors being inspected. *See* CYBERSECURITY REQUIREMENTS RIA, *supra* note 58, at 8.

[172] Inspections should be infrequent. They are not meant to replace DoD cybersecurity assessments already in place, and there is no requirement that every contractor be inspected. To require inspections of all contractors whose cybersecurity systems have not been otherwise assessed would simply add another tier of mandatory assessments, which is not the goal of the inspection process. Instead, inspections should occur when issues are believed to exist and, in other circumstances, with enough regularity that all contractors can reasonably expect the possibility their systems will be evaluated. This corrects issues with contractors with known deficiencies, while motivating honest self-evaluations and corrections in all other contractors, who are aware of the real likelihood they will face an inspection.

existing cybersecurity requirements under the contract, not the inspection process.

Collaborating with in-house cybersecurity experts lifts the DoD over one of the last hurdles it has historically faced when evaluating cybersecurity compliance: the lack of evaluator expertise. With a path towards meaningful inspections and remedies in place, the DoD will finally have effective tools available to motivate serious compliance with cybersecurity requirements.

D. Compiling Performance Data

The DoD can expand the impact of these now-effective inspections by purposefully recording both the results and the remedial measures taken against contractors. The DoD has historically struggled with understanding, even in general terms, the scope of the industrial base's compliance with cybersecurity requirements.[173] At the same time, contractors rarely faced consequences for failing to meet cybersecurity requirements, which has limited their motivation to improve. Both these issues can be resolved in part by actively recording compliance data from the inspection in a way that is useful to the DoD.

Recording inspection data concerning cybersecurity compliance, at the individual contractor level, is relatively straightforward. The entirety of the DoD can record compliance in Contractor Performance Assessment Reporting System (CPARS)[174] performance evaluations. These performance evaluations are the DoD's mechanism for recording "Past Performance Information"[175] and are "used to communicate contractor strengths and weaknesses to source selection officials" for future decisions.[176] Including cybersecurity inspection data in these reports would immediately benefit future source selection decisions by documenting positive or negative information related to the contractor's cyber compliance. It would also significantly motivate the contractor to

---

[173] *See, e.g.*, DOD IG ROI-CONTRACTOR-OWNED NETWORKS, *supra* note 11 (requiring a year-long investigation just to attempt to understand current challenges).
[174] CONTRACTOR PERFORMANCE ASSESSMENT REPORTING SYSTEM, https://www.cpars.gov (last visited May. 8, 2023).
[175] U.S. GEN. SERVS. ADMIN., GUIDANCE FOR THE CONTRACTOR PERFORMANCE ASSESSMENT REPORTING SYSTEM (CPARS) 3 (2022), https://www.cpars.gov/documents/CPARS-Guidance.pdf.
[176] *Id.*

meet all contract requirements in order to preserve its ability to win future DoD contracts.[177]

Importantly, this can be done quickly and cheaply. Adding comments regarding cybersecurity would require essentially no additional resources; these reports are already prepared for all contracts that meet minimum criteria.[178] These comments can also be added immediately. Current regulatory guidance in FAR 42.1503 allows the past performance evaluation to include topics not specifically listed,[179] such as the failure to comply with certain contract terms and conditions.[180]

However, for CPARS comments on cybersecurity compliance to become a regular occurrence, there must be more than just the option to evaluate compliance. There must be an incentive for it to become regular practice among contracting offices. Without regularly including such comments, contractors cannot learn to expect performance evaluations, which lessens the effect of such comments on their motivation to comply, and the DoD will not have sufficient data on past performance to draw meaningful comparisons. The DoD can easily address this concern by requiring their inclusion in CMMC 2.0's rollout.[181]

Notably, inclusion will also help alleviate one of the DoD's biggest problems in addressing the cybersecurity of the defense industrial base: the inability to understand whether problems existed, and, if so, where contractors systemically struggled with compliance and how they could improve.[182] The DoD has taken several significant efforts just to gather one-time snapshots of cyber hygiene data for its use,[183] none of which can produce continuously usable data. That can change now simply by regularly compiling, sharing, and utilizing data from inspection results.

---

[177] *See* FAR 15.305 (2022) (authorizing and detailing procedures for the use of past performance information in proposal evaluations).
[178] *See* FAR 42.15 (2022) (stating when past performance evaluations shall be prepared, how to prepare them, and what contents they should contain).
[179] FAR 42.1503(b)(2)(vi) (2022).
[180] *See id.* (indicating that a contractor's "failure to report in accordance with contract terms and conditions" would be a permissible evaluation factor in a past performance evaluation).
[181] *See About CMMC*, *supra* note 103 (indicating that "[t]he Department [of Defense] intends to pursue rulemaking both in Part 32 of the Code of Federal Regulations (C.F.R.) as well as in the Defense Federal Acquisition Regulation Supplement (DFARS) in Part 48 of the C.F.R" and that "[b]oth rules will have a public comment period").
[182] *See* DOD IG ROI-CONTRACTOR-OWNED NETWORKS, *supra* note 11, at ii (providing an overview of the struggles DoD Component contracting offices to understand the scope of cyber compliance failures amongst contractors).
[183] *See, e.g.*, DOD IG ROI-CONTRACTOR-OWNED NETWORKS, *supra* note 11, at ii (requiring a year-long study to attempt to ascertain issues with cyber compliance in the defense industrial base).

This can greatly alleviate the DoD's effort to gather reliable data as it seeks to improve its programs and understand the challenges its partners face.

IV. Conclusions

The original CMMC framework, through universal third-party assessments, sought to address chronic verification and enforcement issues that plagued the DoD's attempts to improve the cybersecurity of its contractors' networks. While real concerns led the DoD to eventually remove the third-party assessment requirement for the majority of contractors, the return to self-monitoring for those contractors, without additional changes, means that verification and enforcement concerns remain unaddressed. Without the addition of new means of verification and enforcement, it is unlikely that the new framework will lead to meaningful improvements in compliance.

The DoD must address this weakness in current plans by including a means of verifying and enforcing requirements for contractors who self-certify cybersecurity compliance alongside CMMC 2.0. The most effective and efficient way to do so is by adopting regulatory language that allows the DoD a clear means of verification through inspection, along with language providing a practical means of correction and enforcement. With access and enforcement rights clarified, the DoD will still need the appropriate resources to conduct meaningful inspections, but it can do so by utilizing the talent it already has in place. By accurately recording and utilizing inspection results, this verification and enforcement can provide a continuous means of improvement going forward. If the DoD adopts this framework, it will for the first time have a robust set of tools to identify cybersecurity issues, correct failures, and motivate compliance among its self-certifying contractors. If it does not, then the status quo, with its history of widespread noncompliance, will continue.

THIS PAGE INTENTIONALLY LEFT BLANK

THE SECOND KENNETH GRAY & PHYLLIS PROPP-FOWLE LECTURE ON DIVERSITY, EQUITY, AND INCLUSION*

LIEUTENANT GENERAL (RETIRED) FLORA D. DARPINO†

Introduction

I want to thank you all for attending, although I know it is mandatory for some of you. I also want to thank the honored guests that are in attendance: Lieutenant General Stuart Risch, the Honorable Carrie Ricci, and Brigadier General Alison Martin. It is wonderful to see you all. General Nardotti and Susan, it is a special pleasure to see you here. I am going to say that it is truly an honor to speak at the Second Gray & Propp-Fowle Lecture. I never met Lieutenant Colonel Propp-Fowle, but I know she achieved so much in her lifetime. It is amazing to think of the model

* This is an edited transcript of remarks delivered on 28 March 2023 to members of the staff and faculty, distinguished guests, and officers attending the 71st Graduate Course at The Judge Advocate General's Legal Center and School in Charlottesville, Virginia. This lecture is in honor of Major General (Retired) Kenneth D. Gray and Lieutenant Colonel (Retired) Phyllis Propp-Fowle.

† Lieutenant General (Retired) Flora D. Darpino served as The 39th Judge Advocate General of the U.S. Army. She received a direct commission into the Judge Advocate General's Corps in January of 1987. Lieutenant General (Retired) Darpino received a bachelor of arts degree from Gettysburg College in Pennsylvania, a juris doctor from Rutgers University in New Jersey, and a master of laws degree in Military Law from The Judge Advocate General's Legal Center and School. Her military education includes the Senior Service College Fellowship (Department of Justice), the Army Command and General Staff College, the Judge Advocate Officer Graduate Course, Combined Arms and Services Staff School, and the Judge Advocate Officer Basic Course. Her previous assignments include: Trial Defense Counsel and Chief, Civil Law Division, VII Corps in Stuttgart, Germany; Training Officer and Assistant Operations Officer for the U.S. Army Trial Defense Service and Litigation Attorney, Litigation Division, U.S. Army Legal Services Agency; Chief, Administrative Law, 101st Airborne Division (Air Assault) at Fort Campbell, Kentucky; Assistant Executive Officer, Office of The Judge Advocate General; Chief, Judge Advocate Recruiting Office; Staff Judge Advocate, 4th Infantry Division at Fort Hood, Texas and Tikrit, Iraq; Deputy Staff Judge Advocate, III Corps at Fort Hood; Chief, Criminal Law Division, Office of The Judge Advocate General; Staff Judge Advocate, V Corps, in Heidelberg, Germany; Staff Judge Advocate, United States Forces-Iraq, in Baghdad, Iraq; Commander and Commandant, The Judge Advocate General's Legal Center and School; Chief Judge, U.S. Army Court of Criminal Appeals; and Commander, U.S. Army Legal Services Agency.

that she was for all of us. We understand that she paved the way for us, every one of us. Thus, to give a lecture in her name is humbling.

Then, there is General Gray. I met General Gray when I was a second-term captain. I was stationed in Washington, D.C., at the U.S. Army Legal Services Agency (USALSA). I was at the Trial Defense Service (TDS) Headquarters, and General Gray was the USALSA commander at the time. I have a picture of him presenting me with an award where I am very pregnant with my first daughter. I remember him being so kind, and all us captains just adored him. He was warm, engaging, and an inspirational leader. When he was selected to be the Assistant Judge Advocate General with General Nardotti as The Judge Advocate General (TJAG), we, as captains, rejoiced at that leadership team. They led our Corps through a culture change. We talk about being a profession of arms and a profession of law, and it was General Nardotti and General Gray who led that culture change. When I was selected to be The 39th Judge Advocate General, the Deputy Judge Advocate General, Tom Ayres, and I sat down, and we decided that we wanted to do our very best to emulate the team of Generals Nardotti and Gray. That is how inspirational of a leader General Gray was, along with General Nardotti. I hope I do not let him down and make him proud at this second lecture.

I will approach this as I approach most things in my life. First, I'll share anecdotes in old war stories, which is what we do when we get old. But I will also lean heavily on the lessons I learned in my youth from my parents.

Family Upbringing

My parents were children of the Depression, but they were also children of parents that all came from Italy. My father grew up in abject poverty on a farm where they had enough food to feed themselves but not enough to support themselves. My mother grew up in Northern New Jersey, where there was running water and electricity, which they considered a big deal because that meant my father "married up." My father spoke Italian and did not speak English until he attended grade school. He was lucky to graduate from high school; his two older siblings never even graduated from grade school because they had to work on the farm. While my mother had indoor plumbing, she was raised by immigrants who had to work more than one job, as many immigrants do today, to support the family. They worked hard at those jobs. When the Depression hit, it was my grandmother that supported the three of them by working in a weaving mill in North Jersey, where I am sure they locked

all the exits. I do not know if they actually locked the doors, but it was commonplace at the time.

One event changed the trajectory of my family, and that was the G.I. Bill. It allowed my father to go to college. He was sitting in a kitchen with his oldest brother when President Truman announced the G.I. Bill. It could have been as soon as the next morning when my father got in line and enlisted in the Army. I will tell you right now he hated every single minute of it. He never had anything good to say about the Army. So, it is very clear that my father did not inspire me to serve. As Italian Americans who lived through World War II with Mussolini and the Italians on the enemies list, my parents taught us many lessons. I'll mention three in particular: the first was that, in order to be considered equal, we had to be better than those around us. We also could never give anything less than our best. And lastly, we had to remember that people were always watching us. They also stated that each generation had to be better than the generation before them. My mother told us, her daughters, that we had to be strong, independent, and capable of supporting ourselves because we never knew what was going to happen to our spouses. I can honestly say my childhood was more shaped by my Italian identity than it ever was by the fact I was a woman. However, I soon learned the tools my parents gave me worked just as well when I joined a male-dominated profession, the law, in a male-dominated organization, the Army.

Now, some of you may know, my husband and I went to Gettysburg College together and he was a Reserve Officers' Training Corps cadet. We married after law school, at which time I decided to join the military 100 percent so I did not have to take another bar exam. When I told my father, who never had a good day in the Army, that I was joining the Army, he said to me, "Maybe it will be different because you are an officer." Even my father did not realize or take into consideration the fact I was a woman.

Early Judge Advocate General's (JAG) Corps Career

My Officer Basic Course in 1987 was a wonderful experience. There were about twelve women in our class of approximately ninety Soldiers. I was the only married female of the twelve. The JAG Corps was eight percent female, and the highest-ranking women officers were two lieutenant colonels. Of the twelve women or so, I think it is important for you to know four of us stayed on active duty and we achieved some pretty good success. Three of us were division staff judge advocates (SJAs). Then-Lieutenant Colonel Kathryn Stone was the 10th Mountain Division SJA and she deployed to Afghanistan, being the first female division SJA

in an active combat zone. The other two were then-Lieutenant Colonel Sharon Riley, who was the 1st Armored Division SJA, and me as the 4th Infantry Division SJA. Both then-Lieutenant Colonel Riley and I deployed to Operation Iraqi Freedom. The fourth was Lieutenant Colonel Denise Council-Ross, she led a Trial Defense Service region. Out of the twelve women I came in with, the four that remained on active duty rose to some prominent positions, and I find that very impressive. I honestly believe it is because the Schoolhouse set us up for success, even if there were pockets of resistance throughout our careers.

When I reported into my first assignment in April of 1987 at the Trial Defense Service in Stuttgart, Germany, my boss and senior rater said to me, "I asked them not to send me a woman, but they sent you anyway." I know some of you have heard that before and I know what you are thinking. You are thinking that sounds like a setup, but I did not view it that way. The way I viewed it was they, whoever "they" were, decided to "send me anyway." Even though my boss did not want me, they must have reviewed my record and "they" decided that I was capable of doing the job. I was going to prove "they" were right and he was wrong. To do that, all I had to do was lean back on the lessons my parents taught me. I had to be better than the person I worked with and work harder than them in order to be considered equal. I also had to remember they were always watching. And that is what I did in that assignment. I ultimately believe that I was accepted into the organization.

When I went to Germany, I think it is important to note there was still a West and East Germany and there were over 200,000 Army troops in West Germany. It was a big formation with V Corps and VII Corps also present. I later had the privilege to be the SJA of V Corps with my chief paralegal, Command Sergeant Major Noverlette Roberts. Thank you for attending, SGM Roberts. However, that first assignment was not easy. There was sexual harassment and sexual comments regularly in the workplace. It was very common, and I was expected to either accept or ignore it. I have no doubt they believed because their comments were not about me that I should not be insulted. They did not seem to understand that by objectifying and insulting women, they were denigrating me. They did not understand that by saying women did not belong, I believed they thought I did not belong. They did not seem to grasp that by telling me I was the exception and not like the other women that what they were really saying was not a compliment because what that meant was they really did not think being a woman was okay, exceptions aside.

I was raised again to believe I had to prove myself and my equality. I was taught they were watching and judging, and I worked hard in the courtroom and for my clients and refused to be subjugated. Plus, I was not

alone, and I think that is important for you to know. There were the captains, male and female, and we bonded together. We created an incredible supportive team. If one of the sexual harassers was on the road, we would call each other and ensure no woman was alone in the office when they arrived there. When we would go to social events, the male captains would make sure they sat on each side of the women so no idiot would sit next to them.

We viewed the harassers as the outsiders. We believed we represented the real JAG Corps and the Army because, remember, the real JAG Corps and the Army "sent me anyway." Plus, at VII Corps, it was a completely different world. The SJA was Colonel Tom Cuthbert followed by Colonel Walt Huffman, who both became general officers, and represented what we viewed as the real JAG Corps. They measured their officers by their ability. Women were treated as equal members of the team. Even as first-term captains, we understood that Cuthbert and Huffman's type of leadership was the leadership that the JAG Corps and the Army valued because, after all, they were corps SJAs. I finished out my assignment at VII Corps, leaving Germany in April of 1990. The Berlin Wall had been torn down shortly before I left, and I was very pregnant with my first daughter.

Leadership Lessons

Later that fall, Colonel Huffman and his subordinate SJAs readied for Desert Shield and Desert Storm. He asked his subordinate division SJAs to send him their battle rosters. One battle roster only listed men. Colonel Huffman called the subordinate SJA and told him, "Send me a battle roster that includes your best people, not just your men." I believe the conversation ended with something like, "If I don't get a battle roster with your best officers, I believe I will need to find a leader who knows that you take your best into combat." One of the women who was on a battle roster during Desert Shield and Desert Storm is here today and that is Colonel (Retired) Tara Osborn. Thank you for coming, Tara.

I have thought a lot about that first assignment over the years. It was before the Navy Tailhook scandal and an institutional shift in culture. There was no true system of redress. Plus, right or wrong, we believed blending in was better than standing out. However, I did learn some very important leadership lessons that I talked to other officers about through my career.

The first lesson was that you can learn a lot and as much from a bad leader as you can from a good leader. It is equally important to know what

you should not do as it is to know what you should do. The second lesson was it was critical to understand your sphere of influence so you can affect change. We as captains did not have much of a sphere of influence, but we could keep each other safe. The more you rise through the ranks, the greater your sphere of influence and the greater your ability to affect change. Colonel Huffman was able to force change on those battle rosters. And the time may come when you are in a position to implement widespread systemic change. After all, Colonel Huffman did become TJAG and he selected Kat Stone, Sharon Riley, and Flora Darpino, all from my basic course, to be division SJAs. When each of us deployed, we prepared our own battle rosters and we ensured our best people, both men and women, were on them. Sometimes it takes courage to force change and you have to be up to that challenge when you are faced with it.

After my assignment in D.C. and the L.LM program here at The Judge Advocate General's Legal Center and School, I was assigned to the 101st Airborne Division (Air Assault). Shortly after my arrival in 1995, a change in the combat exclusion rule took place. For the first time, women could be assigned to brigade staffs in a combat unit. Prior to that, women could not be down at the brigade in a combat unit. Therefore, there were no women in a combat brigade. At the 101st, each brigade headquarters was staffed with an officer trial counsel and a noncommissioned officer (NCO) paralegal. Only the NCO was on the brigade manning document. Our SJA, Colonel Dave Carey, heard rumblings that not all the brigade commanders were happy about the prospect of having women on their staff. When an opening came up for a brigade NCOIC, Colonel Carey selected his best NCO: an NCO that could run like the wind, climb a rope faster than most, do a punishing amount of pull ups and pushups, and a top-notch paralegal and leader. The NCO also just happened to be female. After she reported into the brigade, word spread quickly, that the commander came flying up to the SJA office complaining about the fact that a woman was being assigned to his brigade. Colonel Carey simply told him, "I only assign my best."

We all know how this story goes. Within a short period of time, that brigade legal office was reported hands down as the best office in the brigade. The NCOIC was indispensable to the leadership team, both as a legal professional and as a leader. Her leadership and office management was commended on a regular basis. Well, the time came for that NCOIC to rotate out of the brigade and word spread quickly throughout the office. The commander came flying back into the SJA's office saying, "You can't take my brigade legal NCO"—the exact same person that did not want her at first. Colonel Carey knew what he was doing when he sent the female NCOIC down to that brigade.

Policy can change, but that does not mean people are ready for change. Colonel Carey used his influence to make sure the right person was assigned to the right job. I suspect when the brigade commander complained, he never came right out and said he did not want a woman. However, if you are leader of change and you are not willing to be complicit, you force them to give voice to their true motives. So, when Colonel Carey looked that commander in the eye and told him that he was sending his best, that left the commander with two choices. At that point, the commander had to say, "I don't want a woman," meaning he was discriminating, or he had to accept that female NCO. I find it highly unlikely that other option where he would say, "I do not want your best" was really an option at all. Colonel Carey forced change and he forced the commander's hand. Honestly, Colonel Carey had full faith in the NCO who he knew was right for the job. Given the opportunity, she changed not only the commander's mind, but the course of legal assignments for the entire 101st.

If you put the right people in the right jobs, they will change minds through their actions. Together, the NCO and Colonel Carey forced change. They made sure she succeeded in the position she earned. Colonel Carey also became a general officer in our JAG Corps and Army, because the Army and JAG Corps value that type of leadership. I left the 101st to attend Command and General Staff College.

Combat Exclusion Rule

After I attended Command and General Staff College, I landed back in D.C. and I was selected for lieutenant colonel. I learned my new assignment was going to be the SJA for the 4th Infantry Division. I heard rumblings that a number of people were upset that I was selected for the job. I was never sure why people were upset that I was selected for the job. I just finished serving two years in TJAG's front office in a lieutenant colonel position as a major. In keeping with what my parents taught me, I worked harder than I could ever imagine and always gave my best. It was at that point I decided I needed to stop listening to the naysayers because maybe those people who were watching were never going to believe I earned my success. So, I wasn't going to listen to them.

I arrived in Texas in June of 2001. On September 11th, I was standing in my sweaty physical training uniform in the chief of staff's office with the chief and the commanding general (CG). We were looking at the television when the plane hit the second tower of the World Trade Center. The CG turned to me and said, "Flora, go get your uniform on." He then

turned to the chief of staff and said, "Assemble the staff." Everything had changed. I felt like I was meant to be in that job, in that division, on that day. I felt like I belonged there.

As we prepared for our deployment in the winter of 2002 and 2003, gender constraints reared its ugly head again. I was minding my own business when I received a call the CG wanted me in the conference room. Never good, right? I knew I had established my reputation on the staff but we all know sometimes a commander and staff can get confused. Sometimes their anger at the law becomes anger at the lawyer. When I went in the conference room, I could actually feel the tension. The division chemical officer related the problem succinctly. He said the regulation, based upon the combat exclusion rule, stated female chemical and engineering officers could be attached to combat units as platoon leaders for training purposes only. The women could not deploy with the units if they went into combat.

We had a number of very successful female platoon leaders serving in both the chemical and engineering companies. At the time, the rule was that women could not serve below brigade staff level, which is why the regulation was written the way it was. The regulation stated the women would have to be pulled from their position when deployed. To exacerbate the situation, there were no male lieutenants to replace the female officers until ROTC graduated in the spring. What that meant was we would be sending these platoons into what we believed was a combat chemical environment without any officer leadership. We knew we had to do a number of river crossings and breaching operations and we would now have engineering platoons without officer leadership.

The division commander, General Odierno, was beyond furious. After a bit of back and forth, I informed him that it is not the lawyer, it is the law. He summarized that the rule resulted in the undeniable conclusion that, somewhere, there was a belief that no officer leadership was better than female officer leadership. General Odierno believed that female officer leadership was every bit as good as male officer leadership. I advised General Odierno to notify higher headquarters of his opinion and to let them know he was taking his platoon leaders. General Odierno, a man who judged every person by their capability, deployed with his female officers leading their platoons. He forced change through necessity. Sometimes change is necessary because the alternative is just plain stupid.

When I deployed, no one on the division staff cared about my gender. They only cared that I was good at my job and that my team was competent and capable. Like every judge advocate, I was pulled into meetings that had nothing to do with law. I was there because I was valued for my analytical skills, creative ideas, problem solving, and common sense. Like

many women and female Soldiers in Iraq and Afghanistan, we were valued members of the team because of our capabilities. I felt as if we had achieved parity.

Then, the summer came, and one by one the female chemical and engineering leaders were replaced by men, even if they had not finished their platoon time. General Odierno had me sit down with each one of those female leaders who had excelled and explain to them the combat exclusion rule to make sure they understood the rule had nothing to do with their ability, performance, or capability. It was a reminder that parity was not actually achieved, and I would need to continue to be vigilant and follow my parents' advice. If I wanted to be considered equal, I needed to continue to work as hard as I could and be my very best every single day. I did that as a lieutenant colonel and as a colonel. I worked extraordinarily hard, always gave my best, and never forgot that they were watching.

Selection as The Judge Advocate General

A number of years later, I was selected and notified I was going to be The 39th Judge Advocate General. Again, I heard rumblings that the naysayers commented I was only selected because I was a woman. I laid in bed for three nights, vacillating between sheer terror that I was going to fail as TJAG and raw anger that folks would think I did not deserve the selection regardless of my gender. I kept thinking that I did not succeed because I was a woman; I succeeded in spite of being a woman. I did not take the place of someone else; I earned my place. And, as always, my husband grounded me with good counsel. He reminded me to ignore the naysayers and approach this job as I have approached every other job in my career. At my promotion, I told the Chief of Staff of the Army, General Odierno, that I would work as hard as I always had, and I would give my best every single day.

While I was TJAG, we dealt with some tough issues and some pretty contentious ones, like the Army downsizing, sexual assault, government shut down, sequester, and operational and international law issues in combat zones. The Army staff did not always agree on every issue, but we implemented the Army vision because that was our responsibility. However, there was one issue we all agreed on. That was eliminating the combat exclusion rule and allowing women to attend Ranger training. I remember someone saying in the room women are already serving in combat roles. General Dempsey really hit this home when he was asked about this question. He told the story of when he was the 1st Armored Division Commanding General in Iraq. He jumped into his gun truck,

tapped the gunner on the leg and said, "Who are you?" The person yelled from the gun turret, "My name is Amanda." The Division Commander was being protected in his truck during that tour by Amanda.

Women were already serving in combat units. They were already walking patrols. They were manning the guns in division commanders' turrets. They were also wounded and killed in combat. As with those chemical and engineering platoon leaders, it was another case of change being necessary because the alternative was just plain stupid. There were vocal opponents to the change, but I think it was important to note the naysayers were not senior leaders in the active Army. Some of the opponents felt allowing women to serve without restrictions would somehow deny positions to men. It seemed they also believed women could not earn these positions under the same standards as men. Another group seemed to believe allowing women in these positions would somehow denigrate a unit or branch's elite status.

All of these naysayers were particularly vocal about Ranger School. Even when the male counterparts of the first female Ranger School graduates publicly stated the women completed every task to the exact same standard or better, they refused to believe it. They just could not simply accept the reality that a woman could earn a Ranger tab. I came to believe there were some men who thought their Ranger tab was worth less because they saw a woman wearing the same tab. Why would a woman accomplishing the exact same thing as a man mean that a man accomplishing that task was worth less? I never truly understood. Unless there are those who believe women can never stand as equals beside them, even if they do the same job. That proposition is not one I am willing to accept.

The most troubling to me were the folks who—I think—believed having women in combat units would somehow make those fighting forces less capable. The women serving in those positions would be required to assess and succeed at the same training as the men. That means they would have demonstrated they were equally capable at the same required tasks as the men. So, how would that make units less capable? I cannot help but remember the women leaders in the chemical and engineering platoons. Those women were assigned to lead those platoons in training, and we train as we fight. Why would we doubt those women would be just as successful in the fight as they were in training? Particularly if their training is the exact same as the men's?

I also believe some were reluctant to change their behavior. I recall addressing a group of non-JAG warrant officers when a chief expressed complete and genuine frustration about the possibility he would have to modify his behavior and speech around women. It was kind of a "boys will

be boys" sort of comment. I simply replied, "You are not a boy anymore. You are an officer and a gentleman. We expect you to act as a gentleman. And as a leader, we expect you to modify your behavior to make a cohesive team and bring out the best in every team member. It does not matter if there is a woman in your formation. The task is the same."

As you know, that is because the Army and the military is a team of teams. And, as a successful team, you need to modify your behavior in order to build bonds and bring out the best in every single member of your team. Strong teams do not objectify. Strong teams do not insult. And strong teams do not degrade each other. Because that tears at the bonds. Instead, strong teams unite and draw out the best in each other, in their capabilities, attributes, and strengths. They work together collectively and push each other to get better. Strong teams are built from each of us being the best people we can be. Women do not change that dynamic. Even in my first office, where my supervisors failed to cultivate that kind of office and that type of cohesive team, we, as captains, united together and we created a strong team that buttressed against the sexual harassment we faced.

In the end, the Department of Defense eliminated the combat exclusion policy even though all members of the Joint Chiefs of Staff did not support it. General Odierno was a strong and vocal supporter of the change. We were also very lucky to have General Dempsey as the Chairman of the Joint Chiefs of Staff. Both men served in combat with female Soldiers. Both of them respected their capability. And both of them knew those women belonged there. I look back at every major juncture of change in my career, and there stood a strong leader who valued people for their abilities. They had the courage to place the right people in the right jobs in order to force change.

Conclusion

Before I joined the Army, they, whoever "they" were, "sent me anyway," and I hope I did not let them down. I did my best. When I was a captain, General Huffman ensured capable leaders who happened to be women were not left out of positions during Desert Shield and Desert Storm. He ensured they were on the battle roster because they earned that spot. When I was a major, Colonel Carey sent down his best NCO to an infantry brigade, knowing she would excel and change the minds of the naysayers. She did change their mind because she was his best and just happened to be a woman. When I was a lieutenant colonel, General Odierno took exceedingly capable female leaders with him to Iraq, in the

positions they had trained for, so their platoons had the leadership they deserved. On the Army staff, when the key domino was teed up and ready to fall, I saw General Odierno and the Army leadership throughout the formation push back against the naysayer noise and the distraction and do what was right for the female Soldiers who deserved it. Those female Soldiers deserved to be treated as full members of the team with full access to success. In each of these pivotal moments, it was leaders who forced the change, and it was the women who made it possible.

I would be remiss without a word of concern about backsliding. When my optimist side tries to make a Pollyanna out of me, I caution myself with a memory of the time when I was the SJA at the 4th Infantry Division. I accompanied General Odierno to a tense meeting with an Iranian dissident group. They were located in Iraq, and for those of you who have been there, they were the Mujahedeen-e-Khalq. Our mission was to have them consolidate both their forces and their arms. The commander of that force, along with all the brigade commanders, sat across the table from us. Each and every one of them was a woman. Every leader in that fighting force was a woman. After two days of sitting across from them in a tug of war of words, they finally agreed to our demands. I then pushed a document across the table to the commander for her signature. She looked me in the eyes, and she pushed that document to her left to the only male sitting on that side of the table. Then, she caught my gaze and said, "I cannot sign a legal document in my own country. Only a man can sign it. That is why I fight. I fight for my equality and my freedom."

I tell you that story because I know those naysayers are still out there. I know they are still looking for opportunities to poke, to prod, and to push back against progress. I still hear comments about the feminization of the military. I still hear comments about how we are weak or weaker because we believe in supporting diversity, equity, and inclusion. You in the Graduate Course, you as leaders, all of us cannot let the naysayers distract us. We have a responsibility to push back on them. Instead, we must continue to push forward and force change. They used the same argument when we tried to integrate race in our service. They used the same argument when we tried to eliminate "don't ask, don't tell." They tried the same argument throughout my career as I watched great leaders force change and people rise to the occasion when they were positioned to succeed. It was because of great leaders that change occurred.

What I remind you as you head back to the field after graduation is that you have the power to force change and you do it through your individual actions. The naysayers fail to recognize that the strength of our Army comes from the combined strength of each and every single one of you. You as leaders, ensure that every member of your team has the ability

to reach their greatest potential. Your responsibility is to make sure that every single one of them has a chance to be their best and the opportunity to reach their full potential. They deserve that as an American Soldier, Sailor, Marine, Airman, Coast Guardsmen, and Guardian. To achieve their full capability and their full potential is a promise that is embedded in the American dream. That is the American dream my parents had for me.

It is now your responsibility as leaders to make sure that each person you lead has that opportunity. Be all you can be. Make sure every person you have the privilege to lead has the ability to be all they can be. I am an American Soldier for life. Thank you.