THE AIR FORCE LAW REVIEW

ARTICLES

VOLUME 70 **2013**

THE AIR FORCE LAW REVIEW

AFPAM 51-106

The Air Force Law Review is a publication of The Judge Advocate General, United States Air Force. It is published semiannually by The Judge Advocate General's School as a professional legal forum for articles of interest to military and civilian lawyers. The *Law Review* encourages frank discussion of relevant legislative, administrative, and judicial developments.

The Air Force Law Review does not promulgate Department of the Air Force policy. The opinions and conclusions expressed in this publication are solely those of the author and do not necessarily reflect the opinion of The Judge Advocate General, The Judge Advocate General's Corps, or any other department or agency of the U.S. Government.

The *Law Review* solicits contributions from its readers. Information for contributors is provided on the inside back cover of this issue.

Readers who desire reprint permission or further information should contact the Editor, *The Air Force Law Review*, The Judge Advocate General's School, 150 Chennault Circle, Maxwell Air Force Base, Alabama, 36112-6418. Official governmental requests for free copies, not under the depository program, should also be sent to the above address.

Cite this Law Review as 70 A.F. L. Rev. (page number) (2013).

Paid subscriptions to *The Air Force Law Review* are available from the Superintendent of Documents, U.S. Government Printing Office, Stop IDCC, Washington D.C., 20402.

Individual copies of this edition may be purchased through the U.S. Government Bookstore at http://bookstore.gpo.gov or by phone at (866) 512-1800 (D.C.-area (202) 512-1800). E-mail: contactcenter@gpo.gov. Fax: (202) 512-2104.

THE AIR FORCE LAW REVIEW

VOL. 70 **2013**

Authority to publish automatically expires unless otherwise authorized by the approving authority. Distribution: members of The Judge Advocate General's Corps, USAF; judge advocates of the Army, Navy, Marine Corps, and Coast Guard; law schools; and professional bar association libraries.

PROTECTING SECURITY AND PRIVACY: AN ANALYTICAL FRAMEWORK FOR AIRBORNE DOMESTIC IMAGERY

Colonel Dawn M.K. Zoldi[*]

[*]Colonel Dawn M.K. Zoldi, USAF (B.A. History and Philosophy, University of Scranton (1989); M.A. History University of Scranton (1989); J.D. Villanova University School of Law (1992); M.S. Military Strategic Studies, Air War College, Air University with Distinction (2010)) is the Chief of Operations Law, Headquarters Air Combat Command, Office of the Staff Judge Advocate. She is a member of the Pennsylvania Bar. The author would like to give special thanks and credit to the following individuals who participated in an informal "Domestic Imagery Working Group," from which the Airborne Domestic Imagery Authorities Matrix, upon which this article is largely based, was drawn: ATSD (IO) (Mr. Michael Goodroe; Mr. Albert Dyson, Mr. Wilbur Snyder); DoD/GC (Mr. Frank Short and Mr. Kyle Jacobson); NGA-OGC (Ms. Allison Stevens and Ms. Jo-Ellen Atkins); SAF/GCM (Mr. Anthony Wager and Maj Monica Nussbaum); JSLC (Lt Col Eric Werner); AFJAGs (Lt Col Richard Dashiell); AF/JAO (Lt Col Lori Coleman and Maj Robert Jarman); ACC A3O (Col Ted Uchida); ACC A2X (Col JudyAnn Wehking); 1AF-AFNORTH (Lt Col Brad Larson and Mr. Curtis "Crash" McNeil); NGB J25 (LTC Andrea J. Johnson-Harvey, MI, ARNG); AFRC/JA (Lt Col Andy Kirkpatrick); Army INSCOM (Mr. Mark D Dupont); 601st AOC (Col Mike Guillory); ATSD(IO); USNORTHCOM (Mr. Bob Hilmo and Maj Patrick Schwomeyer); AFISRA/JA (Col Todd Wold); AFOSI/JA (Lt Col Cindy Stanley); NGB/JA (Col John Joseph and LTC Erin McMahon); 74 ATKW /JA Syracuse ANG (Lt Col Brian Lauri).

I. INTRODUCTION

More than ten years of war in the combat zones of Iraq and Afghanistan have taught a generation of Total Force Airmen valuable lessons about the use of Remotely Piloted Aircraft (RPA)[1] and other Intelligence, Surveillance and Reconnaissance (ISR) assets. The lesson yet to be learned, however, is that this battle space experience is not directly applicable to operations in the United States (U.S.).[2] As the nation winds down these wars, and United States Air Force (USAF) RPA and ISR assets become available to support other combatant commands or U.S. agencies, the appetite to use them in the domestic environment to collect airborne imagery continues to grow, as does Congressional[3] and media interest[4] in their employment. Commanders, operators, intelligence and legal professionals must understand the limited circumstances in which USAF RPAs and ISR assets may be used to collect, process, view, analyze, retain and distribute domestic imagery (DI) consistent with Intelligence Oversight (IO) rules,[5] the Posse Comitatus Act (PCA) and other laws

---

[1] In 2010, the United States Air Force changed the term "Unmanned Aerial Vehicles" (UAV) to "Remotely Piloted Aircraft" (RPA) by institutionalizing RPA pilot training and designating RPA pilots as rated officers (career aviation status). Technical Sergeant Amaani Lyle, *Air Force officials announce remotely piloted aircraft pilot training pipeline*, Air Force News, June 9, 2010, http://www.af.mil/news/story.asp?id=123208561; U.S. Dep't of Air Force, Instr. 11-402, Aviation and Parachutist Service, Aeronautical Ratings and Aviation Badges, 13 Dec. 2010 [hereinafter AFI 11-402,]. This change in terminology is significant in that it recognizes that these vehicles are not "unmanned," but rather are piloted, albeit "remotely," by trained and rated officers. For purposes of consistency, RPA is substituted for UAV throughout.

[2] General Gilmary Michael Hostage III, Commander, Air Combat Command (COMACC), Remarks at Wing Commander's Conference (13 Sept. 2012).

[3] In response to perceived infringements by civilian law enforcement authorities on rights of U.S. citizens, several Bills addressing RPA use were introduced in the 112th Congress. *See* Richard M. Thompson III, "Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses," Congressional Research Service, Feb. 6, 2012, *available at*, http://www.fas.org/sgp/crs/natsec/R42701.pdf.

[4] *See, e.g.*, "Holloman Air Force Base Reaper Rescues Lost Kayakers," UAS Vision Apr. 16, 2012, http://www.uasvision.com/2012/04/16/holloman-air-force-base-reaper-rescues-lost-kayakers/; Mark Mazzetti, "The Drone Zone," New York Times Magazine, Jul. 7, 2012, http://www.realclearpolitics.com/2012/07/07/the_drone_zone_284142.html; Master Sergeant Julie Avey, "163d Reconnaissance Wing Unveils New RPA Hangar," Air Force News, 26 June 2012, http://www.march.afrc.af.mil/news/story.asp?id=123307778.

[5] IO rules govern the collection, retention and dissemination of information on U.S. persons. *See* Exec. Order No. 12333, 3 C.F.R. 200 (1981) [hereinafter EO 12333], *availale at* http://www.archives.gov/federal-register/codification/executive-order/12333.html; U.S. Dep't of Def. Dir. 5200.01 DoD Intelligence Activities (27 Aug. 2007) [hereinafter DoDD 5200.01]; U.S. Dep't of Def Regulation 5240.1, Procedures Governing the Activities of DoD Intel Components that Affect U.S. Persons (1982) [hereinafter DoD 5240.1-R]; U.S. Dep't of Air Force, Instr. 14-104, Oversight of Intelligence Activities, (23 Apr. 2012) [hereinafter AFI 14-104]; *See also* U.S. Dep't of Army, Reg. 381-10 U.S. Army Intelligence Activities, (3 May 2007) [hereinafter AR 381-10], NORAD-USNORTHCOM, Instr.14-3, Intelligence; *Domestic Imagery,* NORAD-USNORTHCOM, Instr.14-103, Intelligence, *Intelligence Oversight*; *available on* the unclassified NORAD-USNORTHCOM Portal to U.S. Government§§ Civilians, U.S. Military members or allies, or contractors supporting military efforts. Register at https://registration.noradnorthcom.mil/

and policies.[6] Although numerous directives, instructions, regulations and policies exist relevant to the most common airborne DI requests in the U.S., determining which guidance actually applies and who can approve a particular mission remains a challenge in some cases. The purpose of this article is to review existing rules and present a comprehensive analytical framework to guide practitioners in obtaining the appropriate level of approval for typical airborne DI requests.[7]

II. THE LEGAL LANDSCAPE

As a general proposition, the Department of Defense (DoD) cannot domestically collect information on non-DoD affiliated individually identifiable U.S. persons (USPER) or organizations using airborne DI or otherwise unless some very specific conditions are met. Yet, at the same time, the DoD has a wide range of national security responsibilities which may require DI collection. The DoD needs to train using DI for combat proficiency, including for combat search and rescue operations. At any given time, and without warning, the DoD may be called upon to give support to civil authorities with DI during crisis situations ranging from hurricanes, to lost hikers, to acts of domestic terrorism. Commanders at local units may need to use DI to protect the people, facilities and equipment under their charge. These examples of potential DI needs are but a few. Given this broad spectrum of operational requirements, the DoD has issued a host of policies and rules that govern this sensitive area. The challenge is to determine which rules apply and when. This is an important determination because the rules designate whether DoD can participate in the mission, whether DoD participation requires a request from an outside agency, which agencies can make the request (and at what level), what DoD capabilities, if any, can be utilized, who can approve DoD participation in the mission and under what constraints. Capability does not equal authority.

The rules applicable to DoD collection of airborne DI are codified in terms of the capability to be used, the mission to be accomplished, or as a combination of both. Below is an overview of the current legal landscape to provide the baseline understanding necessary to analyze a DI request.

---

gateway/Requirements.aspx.

[6] The PCA, 18 U.S.C. § 1385 (1878), restricts direct military assistance for law enforcement purposes except as authorized by the Constitution or Congress. It states, "Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined not more than $10,000, imprisoned not more than two years, or both." For example, the military is generally prohibited from conducting physical surveillance. However, an Intelligence Component can do this for valid counter-intelligence or foreign intelligence purposes under limited circumstances such as physical surveillance of a military member or intelligence employee or pursuant to a valid FISA warrant.

[7] The United States includes the geographic homeland boundaries of the 50 states, the District of Columbia, the territories and possessions of the U.S. to a 12 nautical mile seaward limit of those land areas. AFI 14-104, *supra* note 5 at para. 9.

A. Capability Focused Guidance

The capability focused guidance can be sub-divided into three types: (1) intelligence capabilities; (2) non-intelligence capabilities and (3) RPAs.[8] Executive Order (EO) 12333, *United States Intelligence Activities*, as amended, and its implementing directives and instructions guide intelligence capabilities' collection, specifically collection by Intelligence Components (IC), and by policy extension, Intelligence Component Capabilities' (ICC), on USPER.[9] DoDD 5200.27, *Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense*, applies to non-ICC/ICs collecting information on persons and organizations that are not affiliated with the DoD. In addition, RPAs have their own special rules. These are discussed, in turn, below.

1. Intelligence Components / Intelligence Component Capabilities (ICs/ICCs)

Executive Order (EO) 12333 provides the framework for ICs to conduct intelligence activities, with such activities defined narrowly as countering foreign threats. The goal of the EO, and consequently Intelligence Oversight (IO) in general, is to balance the need for effective intelligence against the "protection of constitutional rights."[10] For this reason, the EO provides strict procedural guidelines for collecting, retaining and disseminating information on USPER.

Under the EO, ICs are only directly authorized to conduct intelligence activities, defined as, "all activities that elements of the IC are authorized to conduct pursuant to this Order."[11] DoDD 5240.01, *DoD Intelligence Activities*, further refines this definition as "the collection, analysis, production and dissemination of foreign intelligence and counter-intelligence (FI/CI) pursuant to EO 12333 and DoDD 5143.01, *UnderSecretary of Defense for Intelligence*."[12]

---

[8] Among intelligence law practitioners, there is no general agreement as to whether or not an RPA should always be considered an "intelligence capability." Some have suggested the RPA's categorization depends on the activity or mission it is conducting at any given moment. Various Speaker Remarks, RPA Lawyer's Group Meetings, (25 Sept, 2012). Regardless, in DoD policies and regulations, RPAs are addressed separately. This article therefore treats such RPA guidance as a special sub-category of capability focused guidance.

[9] EO 12333; *supra* note 5 and AFI 14-104, *supra* note 5 at para. 3.1. According to the EO, USPER "means a United States citizen, an alien known by the intelligence element concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments." EO 12333, *supra* note 5 at para. 3.5(k).

[10] EO 12333, *supra* note 5 at the Preamble.

[11] *Id.* at para. 3.5g.

[12] DoDD 5240.01, *supra* note 5 at Enclosure 2, para. E.2.7. *See also*, EO 12333, *supra* note 5 at Part 2 paras. 2.3 and 2.4. Information is not considered "collected" "until it has been received for use by a DoD IC employee in course of his or her official duties. DoDD 5240.1-R, *supra* note 5 at para. C2.2.1. An "employee" is "a person employed by, assigned or detailed to, or acting for an element within the IC." EO 12333, *supra* note 5 at para. 3.5(d). U.S. Dep't of Def, Dir, 5143.01 UnderSecretary of

Whether through DI or otherwise, when conducting an authorized mission, ICs/ICCs can only collect information on USPER that:

- is obtained with the individual's consent
- is publicly available
- constitutes foreign intelligence or counter intelligence (FI/CI)
- concerns potential intelligence sources or agents
- is needed to protect intelligence sources or methods
- is related to threats to or to protect the physical security of IC-affiliated persons, installations
- is needed to protect intelligence and CI methods, sources, activities from disclosure
- is required for personnel security or communications security investigations
- is obtained during the course of a lawful FI/CI or international narcotics or terrorism investigation
- is necessary for administrative purposes
- is acquired by overhead reconnaissance not directed at USPER and is incidentally obtained that may indicate involving in activities that may violate Federal, state, local or foreign laws.[13]

The approval authority for ICs/ICCs to collect permissible USPER information varies depending on any special collection procedures to be used.[14] For example, in non-emergent situations, electronic surveillance, referred to as a "Procedure 5," may only be conducted pursuant to a warrant under the Foreign Intelligence Surveillance Act of 1978 (FISA). Only the Secretary of Defense (SecDef), Deputy Secretary of Defense (DepSecDef), the Secretary of the Air Force (SecAF) or the Director of the National Security Agency (NSA) can submit a request for a FISA warrant for this purpose.[15]

A DoD IC's failure to follow these stringent procedures or otherwise engage in "questionable activity" which **may** violate the law, any EO, Presidential directive or applicable DoD policy triggers special notification, investigation and reporting requirements to the highest levels of the U.S. government.[16]

Defense for Intelligence, (23 Nov., 2005) [hereinafter DoDD 5143.01], *available at* http://www.dtic.mil/whs/directives/corres/pdf/514301p.pdf.

[13] EO 12333, *supra* note 5 at para. 2.3; DoD 5240.1-R, *supra* note 5 at para. C2.3.

[14] DoD 5240.1-R, *supra* note 5 at para. C5.1.2. *See also*: *Id.* at Procedure 6—Concealed Monitoring, para. C.6.3.3.; Procedure 7—Non-Consensual Physical Searches, para. 7.3.2.; Procedure 8—Mail Searches and Examination, para. 8.3; Procedure 9—Physical Surveillance, para. 9.3.3.; Procedure 10—Undisclosed Participation in Organizations, para. 10.3.2.

[15] To the best of this author's knowledge, SecDef, DepSecDef, and SecAF have never requested a FISA warrant. Rather, the Department of Justice is the one who submits FISA requests in furtherance of CI or FI.

[16] *See* DoD 5240-1R, *supra* note 5. *See also* DepSecDef Directive-Type Memorandum (DTM)

By its terms, the EO and its implementing directives apply to elements of the "Intelligence Community."[17] However, DoD 5240.01-R, *Procedures Governing the Activities of DoD Intel Components that Affect U.S. Persons*, broadens application of IO to non-intelligence organizations, staffs or offices being used for CI and FI.[18] Similarly, AFI 14-104, *Oversight of Intelligence Activities*, applies IO to "*non-intelligence organizations that perform intelligence-related activities* (e.g., Eagle Vision units)[19] that could collect, analyze, process, retain or disseminate information on U.S. persons," including commanders of such units (emphasis added).[20] The National Guard has adopted a similar application of the IO rules to personnel conducting intelligence activities.[21]

08-052—DoD Guidance for Reporting Questionable Intelligence Activities and Significant or Highly Sensitive Matters, (17 June 2009), [hereinafter DTM 08-052], *available at* http://www.dtic.mil/whs/directives/corres/pdf/DTM-08-052.pdf.

[17] For the USAF, the intelligence and counterintelligence (CI) elements which comprise the IC include the AF Deputy Chief of Staff, Intelligence, Surveillance and Reconnaissance; the CI units of the Air Force Office of Special Investigations (AFOSI), Air Force Intelligence Analysis Agency, and "other organizations, staffs, and offices when used for foreign intelligence (FI) or CI to which EO 12333 applies." AFI 14-104, Attachment 1. Note that EO 12333, paras. 1.7 and 3.5(h), outline other IC elements as follows: the Central Intelligence Agency (CIA), Defense Intelligence Agency (DIA), National Security Agency (NSA), the National Reconnaissance Office (NRO), The National Geospatial-Intelligence Agency (NGA), the CI/FI elements of the other Services and the U.S. Coast Guard, the Office of the Director of National Intelligence (DNI) as well as several Interagency Intelligence and CI offices. EO 12333, *supra* note 5 at para. 1.7.

[18] DoD 5240.1-R, *supra* note 5 at para. C15.3.1.3.

[19] Eagle Vision is "a family of deployable, commercial satellite ground stations that downlink unclassified commercial imagery data from Earth-orbiting satellites. Eagle Vision ground system operators - teams that usually run about 12-15 people - can rapidly process that data into a variety of formats within 2-4 hours of collection." Master Sergeant Kate Rust, *Eagle Vision lands at Peterson*, AF News, 18 Nov., 2008, http://www.schriever.af.mil/news/story.asp?id=123124695.

[20] AFI 14-104, *supra* note 5 at para. 3.1. The AFI also applies to "non-intelligence units and staffs when they are assigned an intelligence mission and to personnel doing intelligence work as an additional duty, even if those personnel are not assigned or attached to an intelligence unit or staff" or which operate systems that acquire and disseminate commercial satellite products to intelligence unites and staffs," as well as units and staffs that conduct information operations and cyberspace activities. *Id.* at paras. 3.2.-3.5.

[21] Air Nat. Guard, Instr. 14-101, National Guard Inspector General Intelligence Oversight Procedures, (13 June 2011), [hereinafter ANGI 14-101], *available at* http://www.ngbpdc.ngb.army.mil/pubs/14/angi14_101.pdf. *Id.* at para. 2-3 states, "National Guard requirements. DoD Regulation 5240.1-R reestablishes the requirement for an Intelligence Oversight program in all NG intelligence and intelligence related activities. The procedures apply to the Office of the Chief, NGB, Army and Air NG intelligence units, activities, staffs, and personnel conducting intelligence activities directly related to a federal mission or duty in a Title 10 or Title 32 status. Additionally, the Service components guidance, AR 381-10 and AFI 14-104, further establish requirements for their respective NG elements." *See also* Chief National Guard Bureau Manual 2000.01, *National Guard Intelligence Activities*, (26 November 2012), *available at* http://www.ngbpdc.ngb.army.mil/pubs/CNGBI/CNGBM2000_01_20121126.pdf; Chief National Guard Bureau Instruction 2000.01, National Guard Intelligence Activities, (17 Sept. 2012), *available at* http://www.ngbpdc.ngb.army.mil/pubs/CNGBI/CNGBI.htm.

While the AFI does not define "intelligence-related activities," presumably such activities would be similar to an IC's collection activities using interoperable and compatible intelligence systems, databases and procedures.[22] Thus, while performing intelligence-related activities, the IO rules would apply to ICCs as well as to ICs. The AFI also adds the requirement for a Proper Use Memorandum (PUM) signed at the major command (MAJCOM)[23] level, to define DI requirements, parameters of use and compliance with legal and policy restrictions.[24]

Although not directly codified in the DoDD 5240.01 or DoD 5240.01-R, *Procedures Governing the Activities of DoD Intel Components that Affect U.S. Persons*, the common understanding of IO practitioners is that because ICs/ICCs are only specifically authorized to conduct CI and FI, any other activity or mission requires SecDef approval, with limited exceptions.[25]

2. Non-Intelligence Components / Non-Intelligence Component Capabilities (Non-IC/ICCs)

DoDD 5200.27, *Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense,* limits non-ICs/ICCs

---

[22] AFI 14-104 does, however, define "intelligence activities," consistent with the EO, as "… all activities that DoD intelligence components are authorized to undertake pursuant to Executive Order 12333 and assigns the Services' intelligence components responsibility for: 1, "Collection, production, dissemination of military and military related foreign intelligence and counterintelligence, and information on the foreign aspects of narcotics production and trafficking;" and 2, "Monitoring of the development, procurement, and management of tactical intelligence systems and equipment and conducting related research, development and test and evaluation activities." AFI 14-104, *supra* note 5 at Attachment 1, Terms. *See also* DoDD 5240.01, *supra* note 5 at para. 5.4.2. for the extrapolated definition of ICCs.

[23] A MAJCOM of the USAF is the second highest level of command and reports directly to Headquarters Air Force. *See generally "Air Force Organizational Structure (Chain of Command)," available at* http://usmilitary.about.com/cs/airforce/a/aforganization_2.htm. (last accessed June 23, 2013)

[24] AFI 14-104, *supra* note 5 at para. 9.5, Attachment 1 Terms and Attachment 4. A PUM is not authoritative in nature for the mission it describes. Rather, the PUM outlines how the imagery will be collected retained and to whom it may be disseminated and certifies that such proposed use complies with applicable laws and policies. Independent approval of the mission at the appropriate level is still required. Airborne missions that acquire DI outside of DoD-controlled airspace will also require a Federal Aviation Administration Certificate of Authorization.

[25] One could extrapolate the requirement for ICs/ICCs to obtain SecDef approval for other than CI/FI from the definition of Intelligence Activities in DoDD 5240.01, *supra* note 5 at para. E2.7. ("Intelligence Activities. The collection, analysis, production and dissemination of foreign intelligence and CI pursuant to references (b) and (c)") when read in context of both the directive and the EO it implements. Joint Publication 3-28, Civil Support, (14 Sept. 2007), *available at* http://www.dtic.mil/doctrine/new_pubs/jp3_28.pdf, however, is the only regulation that overtly codifies the proposition that ICs/ICCs are only authorized to conduct CI/FI and all other missions require SecDef approval. In addition to CI/FI, ICs/ICCs are also authorized to conduct training under certain circumstances, as well as activities otherwise approved by SecDef or the President of the United States on an *ad hoc* basis. Remarks by various speakers, RPA Lawyer's Group / Domestic Imagery Working Group Meetings, Sept. 25, 2012 and Nov. 7, 2012, [hereinafter Working Group].

acquisition of information on non-DoD affiliated U.S. citizens to three situations: (1) to protect DoD functions and property (hereinafter referred to as "force protection"); (2) to conduct personnel security investigations and (3) to conduct operations to assist civil authorities during civil disturbances.[26] With the exception of personnel security, these will be further discussed below in the Mission Focused Guidance section.[27]

3. Remotely Piloted Aircraft (RPAs)

In September 2006, the DepSecDef issued a Memorandum, *Interim Guidance for the Domestic Use of Unmanned Aircraft Systems,* which still remains in effect.[28] According to this memo, DoD RPA operations "shall not conduct surveillance on specifically identified U.S. persons, unless expressly approved by the Secretary of Defense, consistent with U.S. law and regulations." AFI 14-104, reiterates this requirement verbatim.[29]

SecDef approval for RPA use is also required for specific missions, including Defense Support to Civil Authorities (DSCA), Military Support of Civilian Law Enforcement Agencies (LEA), Counter-Drug (CD) Operations and National Guard use of DoD RPAs for governor-requested state missions. For training purposes, use of RPAs "outside of DoD-controlled airspace," requires notification to the Chairman of the Joint Chiefs of Staff (CJCS).[30] These missions, including training, will be further discussed below in the Mission Focused Guidance section.

B. Mission Focused Guidance

The mission sometimes lends itself to using airborne assets, whether IC/ICC, Non-IC/ICC or RPA, to acquire DI for a particular purpose. The DoD and the USAF have mission focused regulations that commanders, operators, intelligence professionals, judge advocates and paralegals must consult, in conjunction with the capability focused rules addressed above, to determine applicable approval authorities, procedures, and other guidance. A brief discussion of the relevant

---

[26] Dep't of Def, Dir 5200.27, Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense, paragraphs 2.2.2. and 4.1—4.3(Jan. 7, 1980), [hereinafter DoDD 5200.27], *available at* www.dtic.mil/whs/directives/corres/pdf/520027p.pdf. It is difficult to imagine a scenario where DI would be used in furtherance of a personnel security (aka security clearance) investigation and thus, such investigations will not be further addressed.

[27] It is difficult to imagine a scenario where a Personnel Security investigation will implicate the need to collect DI on a USPER and as such, the subject is beyond the scope of this article.

[28] DepSecDef Memo, Interim Guidance for the Domestic Use of Unmanned Aircraft Systems, (28 Sept. 2006). Regarding the Memo's currency, *see* Remarks by various speakers, RPA Lawyer's Group/Domestic Imagery Working Group Meetings, Sept. 25, 2012 and Nov. 7, 2012. It is the author's understanding that this guidance is pending revision.

[29] AFI 14-104, *supra* note 5 at para. 9.6.2.

[30] DepSecDef Memo, *supra* note 28 at pg. 2.

directives, instructions, regulations and policies for the most common airborne DI missions in the U.S. follows.

1. Defense Support to Civil Authorities (DSCA)

A request from civil authorities for DoD assistance, or independent authorization from SecDef or the President of the United States (POTUS), triggers DSCA.[31] DoDD 3025.18, *Defense Support to Civil Authorities* (DSCA), governs DoD's provision of temporary support to U.S. civilian agencies for "domestic emergencies, law enforcement support, and other domestic activities, or from qualifying entities for special events."[32] The USAF has further implemented DoDD 3025.18 through AFI 10-801, *Defense Support to Civil Authorities*.[33]

The typical approval process for DCSA involves a Request for Forces or Assets from a civilian agency to the DoD Executive Secretary. This request goes up to SecDef, then down to the Joint Staff's Joint Director of Military Support (JDOMS), who sends it to the appropriate Combatant Command as well as to the Services, who then provide the people, equipment or other capabilities needed. For USAF assets or forces, JDOMs will send this request to the Headquarters Air Force, who will likely send it to Air Combat Command (ACC)[34] for the sourcing solution.[35] However, the SecDef has delegated seven specific authorities to the Commanders U.S. Northern Command (CDRUSNORTHCOM) and U.S. Pacific Command (CDRUSPACOM) in the Chairman of the Joint Chiefs of Staff (CJCS) Standing DSCA Execute Order (EXORD).[36] Once SecDef validates the mission from the primary agency in charge of the incident (e.g., Federal Emergency Management Agency or FEMA), USNORTHCOM and USPACOM can provide Incident Awareness and Assessment[37] for:

---

[31] Dep't of Def, Dir 3025.18, Defense Support to Civil Authorities (DSCA), incorporating Change 1, para. 4c., (21 Sept. 2012),[hereinafter DoDD 3025.18], *available at*, http://www.dtic.mil/whs/directives/corres/pdf/302518p.pdf.

[32] *Id.* at Glossary, Part II, Definitions

[33] U.S. Dep't of Air Force, Instr. Defense Support to Civil Authorities (DSCA), (19 Sept. 2012), [hereinafter AFI 10-801], *available at* http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afi10-801/afi10-801.pdf.

[34] ACC is the primary provider of air combat forces to America's warfighting commanders. *See generally, Air Combat Command Fact Sheet*, http://www.acc.af.mil/library/factsheets/factsheet.asp?id=2361. (last accessed June 23, 2013)

[35] DoDD 3025.18, *supra* note 31 at para. 4d and Working Group, *supra* note 25.

[36] An EXORD is, "an order to initiate military operations as directed." Joint Publication 5-0, Joint Operation Planning, Glossary, (11 Aug. 2001), *available at* http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf. Headquarters, Chairman of the Joint Chies of Staff Office, Defense Support of Civil Authorities, (Aug. 14, 2009), [hereinafter DSCA EXORD], *availble at* publicintelligence.net/cjcs-defense-support-of-civil-authorities-dsca-exord/.

[37] The term "Incident Awareness and Assessment" (IAA) is currently not defined in DoD or other policy. Generally speaking, IAA is the use of capabilities to aid the situational awareness of a commander. This could be accomplished using intelligence assets or non-intelligence assets.

- situational awareness
- damage assessment
- evacuation monitoring
- Search and Rescue
  - Chemical, Biological, Radiological, Nuclear and Enhanced Conventional Weapons (CBRNE) assessment
  - hydrographic survey
  - dynamic ground coordination.

Of note, the DSCA EXORD permits USNORTHCOM and USPACOM to request traditional IC/ICC resources to conduct DSCA missions. SecDef approval authorizes the use of IC/ICC capabilities for non-intelligence purposes. However, these missions must be conducted in accordance with IO requirements, including DoDD 5240.01-R.[38]

SecDef has also delegated approval authority for several DSCA events to the Assistant Secretary of Defense for Homeland Defense and America's Security Affairs (ASD(HD&ASA), with the following exceptions: assistance to respond to CBRNE events and civil disturbances, assistance to law enforcement, responding with assets "with the potential for lethality," and any time USAF equipment will be operated under the command and control of civilian authorities.[39]

DSCA normally requires high levels of approval, but when time does not permit the type of coordination discussed above, under "imminently serious conditions," and upon civilian authority request, local commanders may exercise Immediate Response Authority "to save lives, prevent human suffering or mitigate great property damage."[40] Absent higher headquarter direction, the local commander should reassess his or her position at least every 72 hours and terminate the response when the necessity giving rise to it no longer exists.[41] Commanders also have "Emergency Authority" to quell civil disturbances, which will be discussed further below in the section on Military Assistance to Civil Disturbances.[42]

Working Group, *supra* note 25.

[38] DSCA EXORD, *supra* note 36 at paras. BB, 4.B.8, 4.D.7.A, 6.H.3.C., and 9.G.2.A; *See also* NORAD and USNORTHCOM Instruction 14-103, *supra* note 5 at para.2.6. It is the author's understanding that the Standing DSCA EXORD is pending revision.

[39] AFI 10-801,*supra* note 33 at para. 2.1.

[40] *Id.* at para. 1.3.1.3 and DoDD 3025.18, *supra* note 31 at para. 4.g. Immediate Response Authority is not carte blanche for local commanders to provide support to civil authorities. Additionally, in today's communications environment, rarely is there insufficient time to seek approval from higher headquarters.

[41] DoDD 3025.18, *supra* note 31 at para. 4.g(2). However, the likelihood that such communication will not be immediately provided is significantly low given the state of communication connectivity.

[42] *Id.* at para. 4.i.

The DoD Directive on DSCA does not address particular assets or capabilities, with the exception of RPAs. Thus, in this limited manner, the DSCA regulation is both capability and mission focused. It states:

> No DoD unmanned aircraft system (UAS) will be used for DSCA operations, including support to Federal, State, local, and tribal government organizations, unless expressly approved by the Secretary of Defense. Use of armed UAS for DSCA operations is not authorized.[43]

Defense support to civilian law enforcement agencies (LEA) and civil search and rescue (SAR) are forms of DSCA.[44] Discussion follows on the additional regulations and policies that apply to each.

2. Support to Law Enforcement Activities (LEA)

DoD support to Law Enforcement Activities (LEA) is limited by law, including the Posse Comitatus Act, and policy, for fear of military encroachment on civil authority and domestic governance. DoDI 3025.21, *Defense Support of Civilian Law Enforcement Agencies*, provides guidance on the sharing of information collected during military operations, the use of military equipment and facilities, training with LEA, funding and reporting mechanisms for such support.[45] Among other activities, Search and Rescue (SAR), Explosive Ordinance Disposal (EOD), domestic terrorist incident support and Civil Disturbance Operations (CDO) are specifically authorized.[46] The directive also addresses training with LEA in great detail.[47]

Restrictions on DoD support to LEA include many prohibitions including interdicting vehicles, searches and seizures, arrest and similar activities (apprehension, stop and frisk), as well as engaging in questioning of potential witnesses, using force

---

[43] *Id.* at, para. 4.o.

[44] *Id.* at para. 2.c.(5) and U.S. Dep't of Def, Instr. 3003.01, DoD Support to Civil Search and Rescue (SAR), Enclosure 2, paras 2a—2b, (26 Sept. 2011), [hereinafter DoDI 3003.01]. It is worth noting that even though support to law enforcement is a form of DSCA, the CJCS Standing DSCA EXORD does not address it.

[45] U.S. Dep't of Def, Instr 3025.21, Defense Support of with Civilian Law Enforcement Agencies, (27 Feb. 2013), [hereinafter DoDI 3025.21], *available at* http://www.dtic.mil/whs/directives/corres/pdf/302521p.pdf. 10 U.S.C. 371 (1981), Use of information collected during military operations requires that the needs of civilian LEA be taken into account in the planning and execution of military training or operations. *See also* U.S. Dep't of Def, Instr 1322.28, Realistic Miltiary Training (RMT) Off Federal Real Property, (18 Mar 2013), [hereinafter DoDI 1322.28], which incorporates 10 USC 371 requirements; *See also* Secretary of Defense Memorandum, Leveraging Military Training for Incidental Support of Civil Authorities, (11 Dec. 2012), which directs future policy changes to widely implement 10 USC 371.

[46] DoDI 3025.21, *supra* note 45 at Enclosure 3, para. 1.b.(6) and Enclosures 4-6.

[47] *Id.* at Enclosure 3, para. 1.f.; Enclosure 7, paras. 1.d.-f' and Enclosure 9, para. 1.c.

or threats to do so except in self-defense of defense of others, collecting evidence, forensic testing and surveillance or pursuit of individuals or vehicles.[48]

The LEA directive, like the DSCA directive, addresses not only the support to LEA mission, but also use of specific capabilities for that purpose. While the directive generally applies to all DoD assets and capabilities (non-ICs/ICCs), it specifically requires that LEA requests for DoD IC/ICC assistance be processed pursuant to DoDD 5240.1 and DoD 5240.1-R and subject to SecDef approval.[49] While the LEA directive does not directly address use of RPAs, the DSCA directive does and requires SecDef approval.[50]

3. Civil Search and Rescue (SAR)

Civil Search and Rescue (SAR) also constitutes a form of DSCA.[51] It is DoD policy to support civil SAR "to the full extent practicable on a non-interference basis."[52] In fact, DoD personnel are specifically authorized to take actions to provide SAR support domestically under the authorities in the National Search and Rescue Plan.[53]

DoDI 3003.01, *DoD Support to Civil Search and Rescue (SAR)* designates the Commander,USNORTHCOM as the U.S. Inland SAR Coordinator for the

---

[48] *Id.* at, Enclosure 3, para. 1c.(1)(a)—(g).

[49] *Id.* at Enclosure 3, para. 5.b.. SecDef approval is not required for IC's to report potential threats to life and property to appropriate LEAs when "incidentally acquired" during valid intelligence collection activities, in accordance with AFI 14-104, paras. 10.1 and 12. Also, given that the "surveillance" is authorized in Procedure 5 of EO 12333 and DoD 5240.1-R, such duly authorized missions would not violate either the DoDI or the PCA.

[50] DoDD 3025.18, *supra* note 31 at para. 4.o.

[51] DoDI 3003.01, *supra* note 44. SAR is not a "search" within the meaning of the 4th amendment based on the purpose of the search. Although rescinded by DoDI 3003.01, *supra* note 44 DoDD 3003.01, *see* U.S. Dep't of Def, Dir 3003.01, Support to Civil Search and Rescue (SAR), paras. 3.2—3.4, (20 Jan. 2006), *available at* http://www.dtic.mil/dpmo/laws_directives/documents/dodd_3003_01.pdf. This directive provides useful definitions. It defines Civil SAR as "search operations, rescue operations, and associated civilian services provided to assist persons and property in potential or actual distress in a non-hostile environment." A rescue is defined as an "operation to retrieve persons in distress, provide for their initial medical or other needs, and deliver them to a place of safety." A search is "an operation normally coordinated by the Rescue Coordination Center or rescue sub-center, using available personnel and facilities to locate persons in distress."

[52] DoDI 3001.01, *supra* note 44 at para. 4a.

[53] DoDI 3025.21, *supra* note 31 at Enclosure 3, para. 1.b.(6). *See also* National Search and Rescue Pan of the United States (2007), [hereinafter U.S. SAR Plan], *available at* http://www.uscg.mil/hq/cg5/cg534/manuals/Natl_SAR_Plan(2007).pdf and National Search and Rescue Committee, U.S. National Search and Rescue Supplement to the Int'l Aeronautical and Maritime Search and Rescue Manual, (May 2000), [hereinafter NSS], *available at* http://www.uscg.mil/hq/cg5/cg534/manuals/Natl_SAR_Supp.pdf. The U.S. National SAR Plan delineates roles and responsibilities but is not considered an authority to conduct SAR. The U.S. National SAR Supplement is the primary U.S. SAR publication.

Search and Rescue Regions (SRR) that correspond to the 48 contiguous States and CDRUSPACOM, for mainland Alaska.[54] The USAF is the recognized SAR Coordinator for the U.S. aeronautical SRR corresponding to the continental U.S. other than Alaska and in support of that mission, operates the Air Force Rescue Coordination Center (AFRCC) at Tyndall Air Force Base, Florida, to coordinate the conduct of civil SAR operations in those inland SRRs.[55]

When a distress call is received, the AFRCC coordinates with various agencies, including DoD, and requests SAR support.[56] As a practical matter, the AFRCC will directly coordinate at the local unit or wing level and will presume the commander who agrees to have forces respond has the authority to conduct the proposed response with the assets at his or her disposal. Frequently, the commander will respond under Immediate Response Authority, given the nature of the distress call.[57] The DoD SAR directive does not elaborate on such required approvals. However, because inland SAR is considered a form of DSCA, DoDD 3025.18, *Defense Support to Civil Authorities* and AFI 10-801, *Defense Support to Civil Authorities*, also apply. As discussed above in the DSCA section, RPA use for DSCA, including SAR, requires SecDef approval. SAR is also one of the seven delegated authorities in the Standing DSCA EXORD. Therefore, USNORTHCOM and USPACOM may use IC/ICC capabilities for SAR upon SecDef approval. Finally, for civil SAR missions not involving RPA or IC/ICCs, USNORTHCOM and USPACOM authorities, or Immediate Response Authority, ASD(HA&ASA) is the approval authority.

4. Force Protection (FP)

FP is a host-unit commander's responsibility and includes "actions taken to prevent or mitigate hostile actions against DoD personnel…resources, facilities and critical information."[58] Intelligence, including that gleaned from airborne DI, directly supports FP.[59]

Several different regulations address the FP mission, but none directly address the role of airborne DI in support of it. Rather, they discuss the role of

---

[54] DoDI 3001.01, *supra* note 44 at paras. 9a and 10a.

[55] *Id.* at para. 6d.; U.S. SAR Plan, *supra* note 53, and NSS, *supra* note 53.

[56] "Air Force Rescue Coordination Center Fact Sheet," http://www.1af.acc.af.mil/library/factsheets/factsheet.asp?id=7497. (last accessed June 23,2013)

[57] Working Group, *supra* note 25. These approvals include not only authorization from the correct approving official (e.g., SecDef) but also a PUM and, if applicable, FAA COA.

[58] U.S. Dep't of Air Force, Doctrine Doc. 3-10, Force Protection, Forward and Chapter 2, (28 Jul. 2011), [hereinafter AFDD 3-10], *available at* http://www.globalsecurity.org/military/library/policy/usaf/afdd/3-10/afdd3-10.pdf. *See also* U.S. Dep't of Air Force, Instr.14-119, Intelligence Support to Force Protection, para. 1.6, (4 May 2012), [hereinafter AFI 14-119], *available at* http://static.e-publishing.af.mil/production/1/af_a2/publication/afi14-119/afi_14-119.pdf.

[59] AFI 14-119, *supra* note 58 at Terms and para. 1.2—1.3 collectively.

intelligence in anticipating and planning against threats and highlight the importance of complying with IO rules in the domestic environment.[60] AFI 14-119, *Intelligence Support to Force Protection,* provides detailed guidance relating to the role of Force Protection Intelligence (FPI) personnel specifically assigned to support FP through a range of activities, including training, mission planning and threat analysis.[61] In addition to intelligence personnel directly tasked to assist with FP, the regulations anticipate that ICs/ICCs may *incidentally* collect threat information relating to USPER during routine intelligence activities. Both AFI 14-119 and AFI 14-104 indicate that ICs/ICCs who incidentally receive information identifying a USPER as a threat during their routine intelligence activities **must** pass the information to appropriate authorities, in particular the Air Force Office of Special Investigations.[62]

For non-ICs/ICCs, DoDD 5200.27, *Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense*, controls and specifically limits the acquisition of information on non-DoD affiliated persons and organizations in support of FP. Whether acquired through DI or otherwise, the directive circumscribes collecting such information for purposes of protection from the activities below:

- subversion of loyalty, discipline, or morale of DoD military and civilian personnel by encouraging violation of law, disobedience of orders, or disruption of military activities;
- theft of arms, ammunition, or equipment or destruction or sabotage of DoD facilities, equipment, or records; acts jeopardizing security of DoD elements or operations or compromising classified information by disclosure or espionage;
- unauthorized demonstrations on DoD installations; direct threats to DoD military or civilian personnel in connection with their official duties or to other persons who have been authorized protection by DoD resources;
- activities endangering facilities that have classified defense contracts or officially designated as "key defense facilities;" and crimes for which DoD has responsibility for investigating and prosecuting.[63]

None of the regulations that address FP discuss RPAs.

---

[60] AFDD 3-10, *supra* note 58 at pg. 11; Dep't of Air Force, Instr 31-101, Integrated Defense (FOUO), (8 Oct 2009), [hereinafter AFI 31-101], is not publically available.

[61] AFI 14-119, *supra* note 58 at para. 1.6.

[62] AFI 14-104, *supra* note 5 at para.s. 10.1 and 12; AFI 14-119, *supra* note 58 at para. 1.6.9.2. Procedure 12 of DoD 5240.1-R specifically authorizes ICs to provide incidentally acquired information to law enforcement as well as provide direct support, in certain circumstances. DoD 5240.1-R, *supra* note 5 at Procedure 12.

[63] DoDD 5200.27, *supra* note 26 at para. 2.3.

5. Civil Disturbance Operations (CDO)

CDO involves the employment of U.S. military forces to control sudden and unexpected civil disturbances when local authorities are unable or decline to control the situation. The term, "civil disturbances" means, "group acts of violence or disorder prejudicial to public law and order."[64] The significant CDO policy concerns include the primacy of civilian authorities and the use of military force against U.S. citizens in the domestic context.

The authority for CDO derives from the Insurrection Act, which vests decision-making authority in the POTUS.[65] Under DoD policy, military forces shall not be used for CDO unless specifically authorized by the POTUS, except in emergency circumstances. Commanders can provide military assistance using this Emergency Response Authority, "in extraordinary emergency circumstances were prior authorization by the POTUS is impossible and duly constituted local authorities are unable to control the situation, to engage temporarily in activities that are necessary to quell large-scale, unexpected civil disturbances because:

(1) Such activities are necessary to prevent loss of life or wanton destruction of property or to restore governmental functioning and public order or

(2) When duly constituted Federal, State, or local authorities are unable or decline to provide adequate protection for Federal property or Federal Governmental functions."[66]

6. Counter-Drug (CD) Missions

Counter-drug (CD) missions are not considered to be a form of DSCA.[67] CD operations consist of either Detection and Monitoring (D&M) or Aerial Reconnaissance missions (AR) in support of any other federal department or agency or any State, local, tribal, or foreign law enforcement agency for counterdrug purposes.[68]

---

[64] Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, (15 Mar. 2013), *available at* http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

[65] *See* Insurrection Act, 10 U.S.C. 331-335; (1807); DoDD 3025.21, *supra* note 45 at para. 4.1.6.

[66] DoDI 3025.21, *supra* note 45 at Enclosure 3, para. 1.b.(3)—(4) and Enclosure 4, "DoD Support of CDO."

[67] DoDD 3025.18, *supra* note 31 at para. 2.d.(4).

[68] 10 U.S.C. 124, (2004); 10 USC 1004(b)(6), 1004(b)(10) (as amended through the NDAA for FY 2012); 10 USC 371, (1981); 10 USC 374 (1981); Chairman of the Joint Chiefs of Staff Instruction 3710.01B, DoD Counterdrug Support, (26 Jan. 2007); [hereinafter CJCSI 3710.01B]; DepSecDef Memo, Department Support to Domestic Law Enforcement Agencies Performing Counternarcotics Activities, (2 Oct. 2003), *available at* http://www.dtic.mil/cjcs_directives/cdata/unlimit/3710_01.pdf; DepSecDef Memo, Department International Counternarcotics Policy, (24 Dec. 2008).

CJCSI 3710.01B, *DoD Counterdrug Support* vests CD approval authority in the Geographic Combatant Commanders (GCCs) of USNORTHCOM, U.S. Southern Command (USSOUTHCOM), and USPACOM, for specific activities within their respective areas of responsibility; otherwise SecDef is the approval authority.[69] SecDef has, however, delegated his authority to the Under Secretary of Defense (Policy)(USD(P)) and the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict (ASD(SOLIC)).[70] The GCCs can conduct CD missions with the exception of: targeting and tracking vehicles, buildings, persons in the U.S.; providing coordinates to LEAs that is not continuation of a D&M mission; or tracing drug air/surface traffic outside 25 miles inside U.S. territory.[71] These all require USD(P) or ASD(SOLIC) approval.

The CD CJCSI addresses not just the mission, but also specific assets and capabilities, including RPAs, that can be used in support of that mission. GCCs can approve RPA use as well as use of non-RPA and non-IC/ICC platforms for AR but must first determine whether Title 32 National Guard forces can accomplish the mission.[72] For IC/ICCs, if the CD mission equates to CI/FI, Procedure 12 of DoD 5240.1-R, and IO rules, will apply. [73] If the mission is not CI/FI, DoDD 5525.5 will apply and SecDef approval will be required.[74]

7. Training and Exercises

The ability of a Service to train and exercise is derived from the Service Secretaries' organize, train and equip (OT&E) authorities.[75] For this reason, it is commonly understood that within DoD airspace, local unit commanders have wide latitude in conducting training for and with their forces and assets.[76]

AFI 14-104 directly addresses DI in a training context for both non-ICs/ICCs and RPAs:

9.6. Navigational/Target Training activities.

---

[69] CJCSI 3710.01B, *supra* note 68 at Enclosure A, para. 5.a.

[70] DepSecDef Memo, Department Support to Domestic Law Enforcement Agencies Performing Counternarcotics Activities, (2 Oct. 2003).

[71] CJCSI 3710.01B, *supra* note 68 at Enclosure A, para. 1.b.

[72] CJCSI 3710.01B, *supra* note 68 at Enclosure A, paras. 4.a. and 5.a.(4). As a practical matter, NORTHCOM will obtain SECDEF approval for RPA use for CD, per their own internal policy. Working Group, *supra* note 25.

[73] CJCSI 3710.01B, *supra* note 68 at Enclosure A, para. 8.d.

[74] *Id.* at Enclosure A, para. 8.d.

[75] 10 U.S.C. 8013 (2004).

[76] Working Group, *supra* note 25. Even within DoD airspace, a valid PUM should be on file in support of the activity. AFI 14-104, *supra* note 5 at Attachment 4.

> 9.6.1. Air Force units with weapon system video and tactical ISR capabilities may collect imagery during formal and continuation training missions as long as the collected imagery is not for the purpose of obtaining information about specific US persons or private property. Collected imagery may incidentally include US persons or private property without consent. Imagery may not be collected for the purpose of gathering any specific information about a U.S. person or private entity, without consent, nor may be stored imagery be retrievable by reference to US person identifiers. (Added by author: Non IC/ICC)
>
> 9.6.2. Air Force Unmanned Aircraft System (UAS) operations, exercise and training missions will not conduct nonconsensual surveillance on specifically identified US persons, unless expressly approved by the Secretary of Defense, consistent with US law and regulations. Civil law enforcement agencies, such as the US Customs and Border Patrol (CBP), Federal Bureau of Investigations (FBI), US Immigration and Customs Enforcement (ICE), and the US Coast Guard, will control any such data collected. (Added by authority: RPA)

The 2006 DepSecDef Memo titled, "Interim Guidance for the Domestic Use of Unmanned Aircraft Systems," also addresses RPA training:

> Domestic Exercises and Training
>
> > In order to ensure strict observance of executive orders and U.S. law, use of DoD UAS assets in domestic exercises and training requires notification to the Chairman of the Joint Chiefs of Staff if collection systems will be operated outside of DoD-controlled airspace.[77]

[77] DepSecDef Memo, Interim Guidance for the Use of Unmanned Aircraft Systems, p. 2, (28 Sept. 2006), [hereinafter Interim Guidance] The Memo does not define "DoD controlled airspace." The author's proposed definition is that DoD controlled airspace" includes DoD-restricted or warning airspace, designated Military Operating Areas (MOAs), airspace over DoD installations and training areas, airspace owned, controlled or authorized for DoD training activities, including low level training routes. Airborne imaging should be permitted of surface objects located under the lateral confines of DoD controlled airspace, including but not limited to private property, such as vehicles, without consent, so long as there is no intent to target specific U.S. persons. "Operating collection systems outside" of DoD controlled airspace could mean either that the aircraft is being physically flown outside of DoD controlled airspace or its sensors are pointed at and acquiring imagery in surface areas outside the lateral boundaries of that airspace onto non-DoD property.

This guidance reveals two key facts: (1) non-ICCs / non-RPAs can train outside of DoD airspace and view civilian objects for training purposes if in compliance with AFI 14-104[78] and (2) RPA training within DoD airspace is permissible under OT&E authority, and training outside of DoD controlled airspace requires CJCS notification.

With regard to the latter, notifications for RPA training with DI outside of DoD airspace should be sent up to the CJCS through normal chain of command processes, from the Wing, to the Numbered Air Force, to the MAJCOM, to the Service headquarters.[79] Common sense also dictates that the notification should include sufficient information on the activity or event to allow deciding officials to make an informed judgment on its propriety. ACC's Operations Center's Dynamic/ Immediate ISR/Non-Traditional ISR Request (DIIR) Format (8-line Request) For U.S. Missions and Off-Installation Training is a practice worth emulating, particularly in the absence of other guidance.[80] *Ide*ally, a PUM and, if applicable, an FAA Certificate of Authorization would accompany the 8-line, and all of this would be sent through operations channels with sufficient time to account for approvals at all levels.[81]

Approval authority for training with ICs/ICCs outside of DoD controlled airspace remains uncodified. Some argue that since training is not CI/FI, then SecDef approval would be required except when conducted within DoD airspace under command OT&E authority. Some posit that ICCs train for CI and FI, which is their mission, and should be able to do so without SecDef approval.[82] Still others believe that such training would require approval from a Service Secretary.[83] In the absence of clear guidance, the best approach is to coordinate such training with HHQ, who can determine if SecDef approval is required.

In addition to special requirements that apply "outside of DoD controlled airspace," airborne assets used for training in conjunction with ground forces "off federal real property" also have unique approval authorities and notification

---

[78] Compliance with AFI 14-104 would also dictate the need for a PUM and FAA COA, if applicable. Some have advocated that Secretary of the Air Force approval would be required for ICs/ICCs to train outside of DoD controlled airspace, although this is nowhere codified. Interview with Headquarters Air Staff, (10 Jan. 2013) [hereinafter Interview].

[79] Presumably, a comprehensive notification to the CJCS for recurrent events would suffice, and would be re-submitted annually or as deviations are required. Working Group, *supra* note 25. Recall that for USNORTHCOM, however, all use of RPAs requires SECDEF approval, vice CJCS notification, according to their own policies. N/NCI 14-103, para.2.6.

[80] "Modified Requirements Procedure/Battle Drills/Checklists," https://acc.eim.acc.af.mil/org/A3/A3O/A3O3OP/default.aspx. (last accessed June 23, 2013)

[81] Thirty days would be a reasonable amount of time to process RPA training requests to the CJCS. Working Group, *supra* note 25.

[82] *Id.*

[83] Interview, *supra* note 78.

procedures based on the risk associated with the event. DoDI 1322.28, *Realistic Military Training (RMT) Off Federal Real Property*, requires commanders to work closely with their civilian community partners, the media, and keep HHQ closely apprised of RMT events.[84]

As mentioned in the Support to LEA section above, training with airborne assets could occur with LEA. In fact, it is DoD Policy that the military take the needs of civilian LEA be taken into account in the planning and execution of military training or operations.[85]

8. Other Authorized DoD Missions

There are many possible missions besides those noted above, in support of which a commander may desire to use airborne DI capabilities or assets. For example, in support of a major incident resulting in claims against the government, such as a large-scale fire that burns down civilian homes after an aircraft accident, a commander might want to have a full motion video of the damage. Air Force Instruction 51-502, *Personnel and Government Recovery Claims*, authorizes the investigation of such an event, but does not speak directly to aerial photography or video, other than to generally encourage collecting photos or video to adjudicate the claim.[86] This is but one example of other foreseeable uses of aerial DI in support of legitimate USAF missions and objectives, other than those outlined above.[87] Approval authorities in these scenarios will be fact dependent.

III. THE PROPOSED ANALYTICAL FRAMEWORK

The discussion above illustrates the large quantity of directives, instructions, regulations and policies that exist relevant to the most common airborne DI requests. Which rules apply remains a challenge in some cases because the guidance is codified in terms of capability or asset to be used, the mission to be accomplished, or as a combination of both.

---

[84] DoDI 1322.28, *supra* note 45.

[85] 10 U.S.C. 371, (1981); DoDI 3025.21, *supra* note 45; DoDI 1322.28, *supra* note 45; SecDef Memo, *Leveraging Military Training for Incidental Support of Civil Authorities*, *supra* note 45. It is the author's understanding that the final implementation of 10 USC 371, including processes and approval authorities, is still being discussed at the DoD-level, in conjunction with the Department of Homeland Security.

[86] U.S. Dep't of Air Force, Instr. 51-501, Tort Claims, (15 Dec. 2005), [hereinafter AFI 51-501], *available at* http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afi51-501/afi51-501.pdf. The claims video example is merely illustrative and should not be interpreted to indicate that one should expect the claims instruction to address domestic aerial DI. As a practical matter, instead of using aerial DI, a commander could obtain commercially available imagery or seek approval from the Commander Air Forces North (AFNORTH)/First Air Force to have the Civil Air Patrol (CAP) fly an AF-assigned mission. Working Group, *supra* note 25.

[87] It is beyond the scope of this article to address every potentiality.

Whereas Section II discussed the baseline capability and mission focused rules, this next section provides the framework to navigate this labyrinth of guidance and determine the appropriate levels of mission approval, restrictions, mandatory notifications, and other key operational requirements. For example, can the local base commander support a request from local police request to fly his RPA to locate a lost civilian hiker? Can an USAF MC-12[88] unit train by viewing imagery in an in an urban environment off-installation without higher approval? Can a local commander, on his own authority, use an RPA to get a clear picture for force protection when an active shooter is taking shots at the base gate? All of these scenarios are feasible. Despite the volume of guidance available, the answers to the questions posed are not always readily apparent. Who can approve a particular mission and what constraints apply often depends on **both** what kind of capability will be used (IC/ ICC, Non-RPA/Non-ICC or RPA) **and** the type of mission to be accomplished (e.g., training, DSCA, CI/FI, civil SAR, FP, etc.).

The suggested approach is to first determine which capability is to be used (IC/ICC, RPA, Non RPA/Non-IC-ICC) and then look to the specific mission (training, CD, LEA support, CI/FI etc.). This approach, boiled down to its core is: who wants to do what and how do they want to do it? Because the rules for ICs/ICCs are so well defined, a good starting point is to ask whether or not the capability desired to be used is an IC or ICC. If the answer is yes, then, for the most part, unless the activity is CI/FI, SecDef approval will be required and the IO rules will likely apply.[89] If the capability is not an IC/ICC, then practitioners should look to the regulations that relate directly to the proposed mission. Some of these mission-focused regulations contain capability focused guidance. Where they do not, cross-referencing the mission and capability focused guidance will be critical. A thorough discussion of this proposed framework and an illustrative application follows.

A. The Threshold Question – IC or ICC?

The first question to answer is whether or not the capability to be used is an IC or ICC. This is because if the asset or activity is conducted by or with an IC/ ICC, and the mission is **not** CI/FI, then generally speaking, SecDef approval will be required. This is a relatively simple construct which, at first blush, appears easy to apply. It is not. ICs are well-defined. ICCs lack a codified definition.

[88] The MC-12W is a medium- to low-altitude, twin-engine turboprop aircraft. The primary mission is providing intelligence, surveillance and reconnaissance, or ISR, support directly to ground forces. "MC-12 Fact Sheet," http://www.af.mil/information/factsheets/factsheet.asp?fsID=15202 (last accessed June 23, 2013).

[89] SecDef will generally indicate, through a CJCS EXORD, whether or not the IO rules will apply to ICs/ICCs performing non-CI/FI activities, as exemplified by the Standing DSCA EXORD.

1. IC Defined

EO 12333 and its implementing regulations spell out with clarity whether or not something constitutes an IC. In the USAF, the IC consists of its intelligence and CI elements including the AF Deputy Chief of Staff, Intelligence, Surveillance and Reconnaissance, the CI units of the Air Force Office of Special Investigations, the Air Force Intelligence Analysis Agency; and "other organizations, staffs, and offices when used for foreign intelligence (FI) or CI to which EO 12333 applies."[90]

The more difficult issue is determining whether or not an asset or activity is being conducted by or with an ICC.

2. ICC – The "5 Ps" Test

To determine whether an asset is an ICC or whether a non-IC asset is being used as an ICC, for the past twenty years, intelligence law practitioners have been using the "5 Ps" test: People, Pipes, Process, Platforms, and Purpose.[91]

- With regard to "people," the first question to review is: what is the mission of the unit at the time of the activity? Is it an intelligence unit, a training unit, an operational unit, or a different kind of unit altogether?
- When analyzing the "pipes," one must ask: are IC systems being used to collect, retain or disseminate the product? For example, are the products placed on a J2/A2 portal? Do they use an intelligence systems backbone, such as Joint Worldwide Intelligence Communications System, to provide products to clients?
- Regarding "process," where is the information going? Is an IC or its personnel being used to process, analyze, or create products from the data collected?
- When looking at "platforms," determine whether the platform is owned and / or operated by an intelligence unit. If it is not, consider whether or not a non-intelligence platform is being used for intelligence gathering.
- Finally, one must look at the "purpose" of the activity. Is it to gather intelligence? Is it to train? Is it a mission in support of civil authorities?

[90] AFI 14-104, *supra* note 5 at Attachment 1.

[91] Working Group, *supra* note 25. The 5P Test is not codified anywhere other than on the HQ ACC's Domestic Imagery (DI) Authorities Matrix. *See* "HQ ACC's Domestic Imagery (DI) Authorities Matrix," https://acc.eim.acc.af.mil/org/A3/A3O/A3O3OP/default.aspx (last accessed June 23, 2013). This is not an authoritative document.

The answers to the "5P Test" must be viewed holistically, in the context of the time and place of the activity and with the additional overlay of funding (in other words, what funding is used for the people, pipes, processes, platforms?) The reason this test is so critical is that not everything that is in the air that "looks at things" is an intelligence asset, nor is such activity always an intelligence activity or intelligence function. By way of illustration, some might suggest RPAs are, by definition, an intelligence asset. However, RPAs may not always be performing an intelligence activity for purposes of IO rules.[92] The best argument in favor of this proposition is the fact that many of the mission-specific regulations discussed above, such as the DSCA regulation, contain special rules for RPAs. If they were universally considered ICCs, providing this clarification would not have been necessary.

With limited exceptions, ICs/ICCs can only perform CI/FI without SecDef approval—all other IC/ICC activities require SecDef approval.[93] Thus, whether or not an asset or activity is being conducted by or with an IC or ICC is the threshold question for an airborne DI approval authority determination.[94]

B. Step Two – Determine the Mission

If not an IC/ICC, then the next step would be to review the mission focused regulations and policies to determine what they say regarding approval authority, for a particular capability. Imagine if you will, a Matrix, with each mission outlined in down a column, with a row for each potential asset or capability (IC/ICC, RPA, Non-RPA/Non-IC).

1. DSCA

The DSCA directive clearly states that using an RPA for a DSCA mission requires SecDef approval. Likewise, for non-RPA and non-ICs/ICCs, SecDef or ASD(HA&ASA) is the approval authority with limited exceptions: (1) USNORTHCOM or USPACOM CDR is the approval authority when there is a validated Mission Assignment from SecDef and the activity falls within the seven delegated authorities under the Standing DSCA EXORD; or (2) the local unit commander is the approval authority for Immediate Response.[95]

---

[92] Working Group, *supra* note 25.

[93] For example, in accordance with the Standing DSCA EXORD, SecDef approval of listed resources for the seven authorities delegated to CDR USNORTHCOM and USPACOM includes the approval to utilize traditional ICCs to conduct DSCA missions for non-intelligence purposes. Such missions must be conducted IAW DoD 5240.01-R.

[94] The decision authority as to whether or not an activity or asset constitutes an ICC is not codified. Is has been suggested that this determination should be a command decision, made in full consultation with the A3, A2, and JA and documented in some manner. In potentially controversial cases, it has been suggested that coordination occur with HAF A2, A3 and SAF/GC. *See* HQ ACC DI Authorities Matrix, *supra* note 91.

[95] DoDD 3025.18, *supra* note 31 at para. 4.g.,; AFI 10-801, *supra* note 33 at para. 1.3.1.3; DSCA

2. Search and Rescue (SAR)

As civil SAR is a form of DSCA, use of RPAs in support of such a mission requires SecDef approval.[96] Because the USAF AFRCC is the designated SAR Coordinator for the conduct of civil SAR operations in those inland SRRs, requests for civil SAR normally flow through them. As mentioned, the AFRCC will directly coordinate with the host unit for asset availability and presume the local unit has authority and approvals where appropriate. Those approvals, for non-RPA and non-IC/ICCs will track the DSCA regulation requirements. Generally, Immediate Response Authority will apply. Otherwise, ASD(HA&ASA) or SecDef approves the mission. SAR is also one of the seven delegated approval authorities for the USNORTHCOM or USPACOM CDRs under the Standing DSCA EXORD. In summary, if not a designated COCOM mission or an incident giving rise to Immediate Response Authority, either ASD(HA&ASA) or SecDef approval would be required for a local unit to use almost any type of asset in support of civil SAR.[97]

3. Support to Law Enforcement Agencies (LEA)

Non CI/FI support to LEA is also a form of DSCA. For this reason, use of most DoD assets, including RPA, in support of LEA will require SecDef approval.[98] Limited exceptions include SecAF approval, in coordination with ASD (HD&ASA), for DoD personnel to provide training or expert advice; DoD personnel for equipment maintenance; DoD personnel to monitor and communicate the movement of air and sea traffic. Practitioners must carefully consult DoDI 3025.21 for special restrictions and requirements in this area.

4. Force Protection (FP)

Intelligence supports FP and the regulations for ICs/ICCs permit direct support (e.g., "Procedure 12" of DoD 5240.1-R) as well as the ability to pass USPER information incidentally acquired to law enforcement.

For non-ICs/ICCs, DoDD 5200.27, *Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense*, controls

---

EXORD, *supra* note 36.

[96] DoDD 3025.18, *supra* note 31 at para. 4(o).

[97] *See generally Id.*, DoDI 3025.21, *supra* note 45; DoDI 3003.01, *supra* note 44; AFI 10-801, *supra* note 33.

[98] DoDD 3025.18, *supra* note 31 at para. 4(o), states that SecDef approval is required for "UAS" ISO DSCA. *See also* DoDI 3025.21, *supra* note 45 at Enclosure 3, para. 5.a. - d. Declinations of assistance to LEA also need to be submitted to SecDef, through ASD(HA&ASA). SecDef approval is required for non-CI/FI missions for all ICs/ICCs, unless incidentally acquired. DoD 5240.1-R, *supra* note 5 at para. C12.2.2.4.; AFI 14-104, *supra* note 5 at paras. 10 and 12; AFI 14-119, *supra* note 58 at para. 2.7.1.

and specifically limits the acquisition of information pertaining to non-DoD persons and organizations in support of FP, as discussed at length above.

No special guidance exists on use of RPAs for FP, so analysis will require extrapolation from other guidance. Host unit commanders have wide latitude for FP within DoD-controlled airspace and presumably have the authority to use RPA assets in support of FP in that area. However, using RPAs to collect DI outside of DoD-controlled airspace should cause further reflection. DSCA, by definition, occurs off-base and as such, provides a reasonable approach from which to analogize. As use of RPAs for DSCA requires SecDef approval, local commanders should seek to use other assets first and if RPAs are necessary, should seek SecDef approval for FP that uses DI outside of DoD-controlled airspace, in addition to other necessary coordination and approvals.[99] If time does not permit coordination with SecDef, and RPAs are used to collect DI for FP outside of DoD-controlled airspace without prior approval, it has been suggested that, after-the-fact, the local unit commander should submit a DoD 5240.1-R Procedure 15 Questionable Intelligence Activity (QIA) report that: 1) explains why the commander made such a decision (immediate threat to life, limb, mission, government property, etc); 2) articulates how he or she had determined that local civilian LEA elements could not meet the threat requirement (timeliness, capability, etc) or prior approval was not possible; and 3) describe in detail the intelligence or other information that was collected during the mission, particularly anything that could be considered USPER information, and how it was being retained and / or disseminated; and 4) any recommendations for any changes to policy, procedures or training that might be required to better deal with such a situation in the future.[100] This conservative approach presumes that an RPA is an intelligence capability or was used as one in a FP scenario. It is also not codified.

5. Civil Disturbance Operations (CDO)

Regardless of the asset to be used, authority to use military assets and forces to quell civil disturbances rests at the POTUS-level with one limited exception, when a host unit commander invokes Emergency Response authority. As discussed above, Emergency Response is limited to extraordinary emergency circumstances

---

[99] Other coordination and approvals for RPA use for FP outside of DoD-controlled airspace would include the MAJCOM A3 and A2 (for an incident specific PUM), de-confliction with LEA and a FAA COA.

[100] This should be reported immediately as a "'significant or highly sensitive matter'" under DTM 08-052 if any information about the in extremis RPA intelligence activity was going to be disclosed outside of DoD (Congress, media, public, etc.) and might "'impugn the reputation'" of the Intelligence Community/Defense Intelligence Components. This should be reported immediately as a "'significant or highly sensitive matter'" under DTM 08-052 if any information about the in extremis RPA intelligence activity was going to be disclosed outside of DoD (Congress, media, public, etc.) and might "'impugn the reputation'" of the Intelligence Community/Defense Intelligence Components. Email from ATSD(IO) participant from Domestic Imagery Working Group to Author, (Nov. 11, 2012), providing informal and personal opinion, not binding on ATSD(IO), which is on file with the author.

where prior authorization by the POTUS is impossible and duly constituted local authorities are unable to maintain control.[101]

6. Counter-Drug (CD) Missions

The applicable directives and policies permit GCCs to use RPAs and non-RPAs / non-ICCs for CD missions except to target and track vehicles, buildings, persons in the U.S., to provide coordinates to LEAs that is not continuation of D&M mission, or for drug air/surface traffic outside 25 miles inside U.S. territory. GCCS are also permitted to conduct aerial reconnaissance missions. SecDef has delegated his approval authority for all other CD ops to USD(P) and ASD(SOLIC), with the exception of using ICs/ICCs for non-CI/FI CD ops.[102] Using Title 32 forces for these missions is a DoD priority.[103] The take-away for local unit commanders is that they will not conduct CD missions except through a valid COCOM or Headquarters Air Force tasking, the latter through the MAJCOM.[104]

7. Training

Within DoD-controlled airspace, pursuant to OT&E authority, local unit commanders have wide latitude in acquiring DI for training with virtually any asset, whether IC/ICC, RPA or non-ICC/non-RPA.[105] ICs/ICCs training outside of DoD controlled airspace require, at a minimum, discussion with the MAJCOM, as approval authority to do so is not codified. RPA training that involves acquiring DI outside of DoD airspace requires CJCS notification.[106] Non-ICs / ICCs can train outside of DoD airspace and view civilian objects for training purposes in compliance with AFI 14-104.[107] Aviation assets used in conjunction with ground forces who are operating "off federal real property" also have special approval authorities and notification requirements, depending on the risk level of the event.[108] Finally, military planners should take LEA needs into consideration for any training or operation.[109]

---

[101] DoDI 3025.21, *supra* note 45 at Enclosure 3, para. 1.b.(3)—(4) and Enclosure 4.

[102] CJCSI 3710.01B, *supra* note 68 at Enclosure A, paras. 5.a. and 1.b.; DepSecDef Memo, *Department Support to Domestic Law Enforcement Agencies Performing Counternarcotics Activities*, *supra* note 70.

[103] CJCSI 3710.01B, *supra* note 68 at Enclosure A, para. 5.a.(4).

[104] The Services may further delegate their authority to support Joint Task Forth-North (JTF-N) CD missions, but local units should work through their MAJCOM on any request for support to a CD operation. *See* CJCSI 3710.01B, *supra* note 68 at Enclosure A, para. 5.a.(5). *See also* 10 USC 1004(b)(6), 1004(b)(10) (as amended through the NDAA for FY 2012); 10 USC 371, (1981); 10 USC 374, (1981).

[105] 10 U.S.C. 8013, (2004).

[106] Interim Guidance, *supra* note 77 at p. 2.

[107] AFI 14-104, *supra* note 5 at para. 9.6. Compliance with the AFI dictates the use of a PUM.

[108] *See generally*, DoDI 1322.28, *supra* note 45.

[109] 10 U.S.C. 371, (1981); DoDI 3025.21, *supra* note 45; DoDI 1322.28, *supra* note 45; SecDef Memo, *Leveraging Military Training for Incidental Support of Civil Authorities*, *supra* note 45.

8. Other Authorized DoD Missions

Approval authorities in situations other than those delineated above will be fact-dependent. Use of an IC/ICC capability for something other than CI or FI would require SecDef approval. Using other assets remains uncodified. As in the case of other situations that lack specific guidance, we turn to existing guidance by analogy. It may be safe to assume given the special guidance relating to RPAs in current regulations, that, as a matter of policy, using an RPA to collect DI outside of DoD-controlled airspace for an authorized DoD mission other than those discussed above, would require SecDef approval. As a general matter, the approval authority to use a non-IC/ICC or RPA outside DoD airspace is less clear, but arguably more permissive.[110]

C. The Framework Applied

To illustrate how the proposed framework applies, consider the following hypothetical situation.

1. The Facts.

In MC-12 Initial Qualification Training, non-intelligence personnel are trained on sensor operations to enable them to track terrorists during combat operations. As part of the training, the trainees acquire full motion video, but this video only feeds into a mock training Operations Center during the flight, is retained for classroom use (DoD only audience) for 24 hours and is then deleted. The airframe used is not a real MC-12, but rather a civilian mock-up with a sensor ball commercially purchased with operations (not intelligence) funding. During training "missions," the planes fly primarily on the military base, but can turn their sensor ball to areas outside of DoD controlled airspace and property. Adjacent to the base, civilian-inhabited areas in the sensor range include a local trailer home park, a public park and two state highways.

During one particular training sortie, as the trainees are uneventfully tracking a pre-positioned DoD vehicle on the base's training range, they are told by their military instructors to divert their sensors to a particular house in a trailer park and watch a particular individual at his car and as he entered the house. The crew does this, monitors the situation and reports what they see back to their military instructors at the training Operations Center. Their report includes that the individual appeared to take a small package out of the back seat and bring it into the house. The trainees next see the local police arrive and arrest the individual.

[110] *See* AFI 14-104, *supra* note 5 at para. 9.6. by analogy (permissive use of non-RPA / non-ICCs off base for training).

Behind-the-scenes, the local police had called the training instructors, given their great relationship, and asked them to use the training mission to assist them in a drug bust. The instructors agreed and directed the students to provide them information, which they, in turn, fed back to the local police.

2. The Analysis.

The first question to answer is whether or not the activity in this case, an operational training sortie by non-intelligence personnel in a mock-up MC-12 with a commercial sensor, constitutes activity of an IC. In the USAF, the IC consists of its intelligence and CI elements including the AF Deputy Chief of Staff, Intelligence, Surveillance and Reconnaissance, the CI units of the Air Force Office of Special Investigations, the Air Force Intelligence Analysis Agency; and "other organizations, staffs, and offices when used for foreign intelligence (FI) or CI to which EO 12333 applies."[111] Because the trainees and equipment were not part of these offices and agencies, they are not part of the IC.

The next issue is to determine whether or the MC-12 mock-up asset under these circumstances constitutes either an ICC or a non-IC asset used as an ICC, using the "5 Ps" Test: People, Pipes, Process, Platforms, and Purpose.[112]

With regards to People, the mission of the unit at the time of the activity was a training unit. The people involved were non-intelligence personnel.

The Pipes, in this case were not IC systems. No IC systems were used to collect, retain or disseminate the full motion video. The information flowed through a system purchased with operational funds.

The Process involved streaming information live into a training Operations Center and holding it only 24 hours for training purposes for a DoD audience. No IC or IC personnel were used to process, analyze, or create products from the data collected. However, military training instructors verbally disseminated the information to civil authorities when they relayed what they saw on the video to the local police.

The Platform was not owned or operated by an intelligence unit. As mentioned, a training unit was involved in this scenario. However, in this case, it appears that a non-intelligence platform (the MC-12 mock up with commercial sensor) was used for intelligence gathering. Specifically, the training crew targeted

---

[111] AFI 14-104, *supra* note 5 at Attachment 1.

[112] Working Group, *supra* note 25. The 5P Test is not codified anywhere other than on the HQ ACC's Domestic Imagery (DI) Authorities Matrix. *See* "HQ ACC's Domestic Imagery (DI) Authorities Matrix," https://acc.eim.acc.af.mil/org/A3/A3O/A3O3OP/default.aspx (last accessed June 23, 2013). This is not an authoritative document.

what appears to have been a USPER with their sensor and reported information on his activities back to the training Operations Center, who in turn, provided the information to local law enforcement.

Initially, the Purpose of the activity was to train future MC-12 sensor operators to perform a combat ISR function, which, by definition is a combined intelligence and operational function. However, when the military instructors directed the trainees to point their sensor at a USPER, monitor and report back on his activities, the purpose of the mission changed from one of training *qua* training to intelligence gathering. Despite the training value in this monitoring activity, once the information gathered was passed to and in support of civil authorities, it became an intelligence activity.

Holistically, in the context of the time and place of the activity, the MC-12 mock up with commercial sensor and operational training crew constituted a non-IC asset used as an ICC.

With limited exceptions, ICs/ICCs can only perform CI/FI without SecDef approval; all other activities require SecDef approval.[113] DoDD 3025.21, *DoD Support of Civilian Law Enforcement Agencies*, provides the seminal guidance for DoD support to civilian law enforcement.[114] It also specifically requires that LEA requests for DoD IC/ICC assistance be processed pursuant to DoDD 5240.1 and DoD 5240.1-R and subject to SecDef approval.[115] The military instructors in this case directed their trainees to take action for which they had no authority.

Under these facts, the local commander would have to report this incident as a questionable intelligence activity under DoD 5240.1- R (Procedure 15) and DTM 08-052, through channels, to ATSD(IO).

3. The Key Take-Aways

Hopefully, this application of the proposed framework also illustrates that it works as a reasonable means to approach domestic DI issues. Application of the framework should assist legal practitioners in advising commanders and operators

---

[113] For example, in accordance with the Standing DSCA EXORD, SecDef approval of listed resources for the seven authorities delegated to CDR USNORTHCOM and USPACOM includes the approval to utilize traditional ICCs to conduct DSCA missions for non-intelligence purposes. Such missions must be conducted IAW DoD 5240.01-R. DSCA EXORD, *supra* note 36.

[114] U.S. Dept't of Def, Dir. 5525.5, DoD Cooperation with Civilian Law Enforcement Officials, (20 Dec. 1989), [hereinafter DoDD 5525.5], *available at* http://www.dtic.mil/whs/directives/corres/pdf/552505p.pdf.

[115] *Id.* at paras. E3.4.3.2. and E4.5.3.4. SecDef approval is not required to the IC's mandatory requirement to report potential threats to life and property to appropriate LEAs when "incidentally acquired" during valid intelligence collection activities, in accordance with AFI 14-104, paras. 10.1 and 12. Also, given that the "surveillance" is authorized Procedure 5 of EO 12333 and DoD 5240.1-R, such duly authorized missions would not violate either DoDD 5525.5 or the PCA.

to make informed judgments as to the proper approval authorities and constraints on action. In a perfect world, the analysis and concomitant discussions would occur well in advance of a proposed mission.

There are several other learning points to be gleaned from this scenario. The first truism is that in the real world, the issues practitioners in this field will confront will be just as complex… and never easy. Another teaching point is that mistakes will happen, and when they do, report as required. Finally, a key lesson from the scenario, and this article in general, is that command authority to use DI *sua sponte* in the domestic environment is limited. With the exception of training within DoD controlled airspace, approvals for most missions reside at the SecDef level.

IV. CONCLUSION

Commanders, operators, intelligence professionals and legal professionals need to understand that using RPA and ISR assets to acquire airborne imagery in the domestic environment is different from what they may be accustomed to in an operational combat environment. Numerous directives, instructions, regulations and policies apply to properly employing these assets in the U.S. While the guidance is plentiful, it is not always directly on point. As a result, pinpointing who can approve a particular mission sometimes remains a challenge. Getting it right is critical, however, because failing to do so can have significant consequences that negatively impact the USAF's credibility and otherwise detract from the legitimacy of our operations.

This article reviewed the existing guidance, capability and mission focused, and proposed a comprehensive analytical framework to navigate and cross-reference these two different sets of rules. The proposal, boiled down to its core is: who wants to do what and how do they want to do it? The approach suggested was to first determine which capability is to be used and then look to the specific mission and where the guidance remains murky, extrapolate based on analogous guidance. This common sense approach should assist commanders, operators, intelligence and legal professionals understand the rules for collecting DI and how to apply them to ensure mission accomplishment, consistent with the law.

THE SKY HAS NOT FALLEN: A BRIEF LOOK AT THE IMPACT OF UNITED STATES V. WALTERS TEN YEARS LATER

Lieutenant Colonel W. Shane Cohen[*] *and Captain Jonathan S. Sussman*[**]

[*]Lieutenant Colonel Cohen is currently assigned as a Military Judge, Air Force Trial Judiciary, Western Region, Travis Air Force Base, California. In this capacity, he serves as a trial judge at general and special courts-martial, legal advisor for officer discharge boards, and investigating officer for judicial investigations under Article 32, UCMJ.

[**]Captain Jonathan S. Sussman is an Assistant Staff Judge Advocate for the 35th Fighter Wing at Misawa AB. He is presently Chief of Operations and International Law. Prior to his current position, he held multiple positions at the 355th Fighter Wing at Davis-Monthan AFB, Arizona. He is a former adjunct faculty member at the University of Arizona School of Government and Public Policy where he taught courses in law, public policy and Government bureaucracy.

I. INTRODUCTION

Ten years ago the United States Court of Appeals for the Armed Forces, (CAAF) decided *United States v. Walters*.[1] Notwithstanding the initial angst among military practitioners after the opinion was issued, the day-to-day court-martial practice has not changed much since then. Despite the immediate fear that the use of "divers occasions" had seen its last days and prosecutors would need to break out every offense charged, no matter the difficulty in doing so, the sky has not fallen since *Walters* and is unlikely to fall anytime soon. In fact, the use of the term "on divers occasions" is just as alive today as it was ten years ago. Moreover, the 2012 edition of the Manual for Courts-Martial still lists the term as a valid means of drafting specifications.[2] Although much ado was made about the *Walters* decision and its potential impact, a look at the progeny of the *Walters* case shows otherwise. Both trial practitioners and the appellate courts have narrowly applied the holding in *Walters*, focusing on the ability to do a factual sufficiency review on appeal and not the legitimacy of charging "divers occasions." This article briefly reintroduces *Walters*, tracks the history of several cases since *Walters*, explains the reasons why the holding remains narrow, and then attempts to highlight the various reasons why charging "on divers occasions" remains a valid and practical decision in modern court-martial practice.

II. *UNITED STATES V. WALTERS*

In order to understand the angst surrounding *Walters*, begin with the case itself. In *Walters*, the accused was charged, inter alia, with wrongful use of ecstasy "on divers occasions between on or about 1 April 2000 and on or about 18 July 2000." In returning a guilty verdict for a single use of ecstasy,[3] the members had

---

[1] 58 M.J. 391 (C.A.A.F. 2003).

[2] *See* MANUAL FOR COURTS-MARTIAL, UNITED STATES, R.C.M. 307 discussion (2012) [hereinafter MCM].

[3] Walters, 58 M.J. at 392-394. ("Appellant was tried by general court-martial for one specification of wrongfully using and one specification of wrongfully distributing ecstasy in violation of Article 112a. A panel of officer and enlisted members found him not guilty of the wrongful distribution specification; accordingly, that specification is not at issue in this appeal. The wrongful use specification alleged use 'on divers occasions between on or about 1 April 2000 and on or about 18 July 2000.' The Government offered proof at trial of a number of instances of alleged use of ecstasy during the time period in the specification:

> (1) Senior Airman (SrA) Russ, a friend of Appellant's who testified throughout the trial under a grant of immunity, spoke about an occasion in middle to late June 2000 when Appellant told him that he had used ecstasy. [SrA] Russ testified that at the time Appellant's eyes were glassy, his pupils looked dilated and he was twitching and making strange gestures.
> (2) A friend of Appellant, Airman First Class (A1C) Humble, testified about an occasion at some point between March 3, 2000 and July 31, 2000 where Appellant made a statement that he was planning on using ecstasy.
> (3) An undercover special agent for the Air Force Office of Special Investigations testified that on June 23, 2000 Appellant told her that he had taken a pill of ecstasy

excepted the words "on divers occasions," but failed to identify the specific use for which they had convicted the accused. Nor had the military judge instructed the court members that they would need to specify which instance had been agreed upon by the members.[4] Consequently, on appeal the Appellant argued that the findings of the court were vague, ambiguous and failed to indicate what facts constituted the offense.[5] After taking a look at the case, CAAF agreed and pointed out that "[a] Court of Criminal Appeals cannot find as fact any allegation in a specification for which the fact-finder below has found the accused not guilty."[6] Consequently, CAAF reversed the decision of the lower court, set aside the conviction, and dismissed the charge and specification.[7]

So, why all the anxiety immediately following the ruling? Much of the initial concern stemmed from an overly broad reading of the *Walters* decision and its implications. Some felt that *Walters* indicated CAAF was taking a negative view of the practice of charging multiple offenses as "divers occasions." However, such a view has been shown over time to be without merit. In *Walters*, the only issue CAAF was addressing was whether or not an appellate court could conduct a factual sufficiency review when the term "on divers occasions" had been excepted and the fact-finder had not indicated which fact or allegation was found to have constituted the singular offense. In fact, had the military judge simply instructed the members to indicate which allegation formed the basis of the finding of guilty, the *Walters* decision likely never would have been issued. Nevertheless, for several years

---

"an hour or two ago." She testified that he was perspiring, his speech was slurred, and his skin was sensitive to the touch.

(4) [A1C] Humble testified that sometime between March and July 2000 Appellant was in Humble's dorm room with [Appellant's] girlfriend. [A1C] Humble testified that Appellant said it was his first time using ecstasy and he wanted his girlfriend to try it with him. [A1C] Humble also testified that he observed Appellant pull a piece of plastic out of his pocket that appeared to contain a couple of small pills and that Appellant appeared to hand something to his girlfriend.

(5) [SrA] Russ testified that he was in A1C Humble's dorm room at some point around July 4, 2000 when they were joined by Appellant and his girlfriend. [SrA] Russ indicated that he observed Appellant taking what appeared to be small pills out of his pocket in a plastic wrapper, at which point A1C Humble and Appellant had a "little argument" and Appellant left with his girlfriend, returning thirty to forty-five minutes later.

(6) [SrA] Russ also testified that Appellant came into his [SrA Russ'] room in July of 2000 with two pills wrapped in cellophane. [SrA] Russ testified that Appellant asked him if he wanted to crush one of them, which SrA Russ did. [SrA] Russ testified that Appellant swallowed one of the pills and used a dollar bill to "snort" the crushed pill. In addition to observing a mood change on Appellant's part, SrA Russ testified that he applied Vick's VapoRub[®] to Appellant's face and observed Appellant smoking menthol cigarettes, both alleged to enhance an ecstasy high." *Id.*).

[4] *Id.* at 393-394.

[5] *Id.* at 394.

[6] *Id.* at 395.

[7] *Id.* at 397.

following *Walters*, many practitioners and legal scholars advocated for minimizing the use of the term "divers occasions" or getting rid of it altogether. Although such approaches are authorized and may even be preferable in certain situations, the validity and practicality of using "on divers occasions" still remains, and the post-*Walters* cases have done nothing to indicate the appellate courts are trying to do away with it.

III. THE PROGENY OF *WALTERS*

As the *Walters* court explained, the courts of criminal appeals have the awesome power of factual sufficiency review. "This unique power of review for factual sufficiency, however, is subject to a critical limitation. . . . Without knowing which incident that Appellant had been found guilty of and which incidents he was found not guilty of, that task is impossible."[8] Indeed the early cases after *Walters* have supported this notion. This portion of the article will explore how the W*alters* progeny has addressed special findings and general verdicts.

A. Excepting "Divers Occasions" Requires Special Findings

In *United States v. Augspurger*, the accused was charged with wrongfully using marijuana "on divers occasions." The members found him guilty of only a single use, and not guilty of use "on divers occasions." In doing so, the members failed to indicate which of the three alleged uses formed the basis for its finding. CAAF overturned the conviction, finding the appellate court could not conduct a factual sufficiency review of the conviction because the military judge failed to clarify the factual basis upon which the members' findings of guilty and not guilty were based. The Court explained, "when a servicemember is charged with illegal conduct 'on divers occasions' and the members find the accused guilty of charged conduct but strike out the 'on divers occasions' language, the effect of the findings is that the accused has been found guilty of misconduct on a single occasion and not guilty of the remaining occasions."[9] The Court further noted that the military judge is responsible to ensure that any ambiguities are clarified before findings are announced and, if the judge fails to do so "the appellate courts cannot rectify the error."[10]

---

[8] *Id*. at 395–396.

[9] United States v. Augspurger, 61 M.J. 189, 190(C.A.A.F. 2005).

[10] *Id.* at 193 (opining that the military judge had two opportunities to ensure that the members' findings, as announced, were clear the Court stated: "First, she should have properly instructed the members that if they excepted the 'divers occasion' language they would need to make clear which allegation was the basis for their guilty finding. Second, after she examined the findings worksheet but prior to announcement, the military judge should have asked the members to clarify their findings." *Id*. at 192).

United States v. Ross involved a charge for the possession of child pornography. When entering findings, the military judge excepted the words "on divers occasions," and found the accused not guilty of the excepted words but guilty of the remaining language.[11] The court of criminal appeals affirmed the conviction. On appeal, the Government relied on *United States v. Simmons* to argue that the judge only removed the "divers language" because he was obligated to do so in continuing offenses, that the "divers language" was simply surplusage, and "striking these words did not render the findings ambiguous."[12] CAAF disagreed that this was a clear instance of a continuing course of conduct and concluded that the reason for the judge's removing the "divers language" was unclear. Consequently, CAAF overturned the conviction. In doing so, the Court stated, "[T]he fact remains that we cannot know, nor could the CCA know, what the military judge found Appellant guilty and not guilty of, or indeed whether he found Appellant not guilty of anything at all."[13]

On the other hand, some cases decided after *Walters* have confirmed the narrowness of its holding. For example, in *United States v. Scheurer* the accused was charged with several specifications of drug use, one of which was upheld despite removing divers occasions language, without special findings, because the facts lent themselves to no other conclusion but that one particular factual basis accounted for the conviction.[14] As drafted, the original specification stated that the Accused "'did, at or near Tokyo, Japan, and Mt. Fuji, Japan, on divers occasions between on or about 1 April 2000 and on or about 31 July 2000 wrongfully use lysergic acid diethylamide (LSD).'"[15] The judge removed the phrase, "'and Mt Fuji, Japan, on divers occasions,'"[16] and found the accused not guilty of the excepted words. The evidence showed that the accused's drug use was limited to only two occasions. On review, CAAF upheld the specification, noting that when the military judge excepted the language "and Mt. Fuji, Japan on divers occasions" from the specification, he was necessarily finding the accused guilty of the only other use.[17] Thus, even if special findings are not made, the appellate court can still uphold the conviction if it is readily apparent upon which of the factual scenarios the conviction is based.

---

[11] United States v. Ross. 68 M.J. 415, 415 (C.A.A.F. 2010).

[12] *Id*. at 417; *See also* United States v. Simmons, 37 M.J. 36, 36 (C.M.A. 1992)(dealing with the issue of "at divers times" being surplusage because the possession of marijuana over a twenty day period was a continuing offense.)

[13] *Ross*, 68 M.J. at 418. However, the Court did not overturn Simmons, thereby leaving the "continuing offense" option available for future debate.

[14] United States v. Scheurer, 62 M.J. 100, 110-111 (C.A.A.F. 2005).

[15] *Id*. at 111.

[16] *Id*. at 112.

[17] *Id*.

B. Notwithstanding *Walters*, General Verdicts Still Authorized in "Divers Occasions" Cases

In a case note from 2008, two learned authors raised the following concern regarding charging "divers occasions" post-*Walters*:

> Consider the following hypothetical: suppose an accused is charged with committing misconduct 'on divers occasions,' and the trial counsel puts forth evidence of five separate incidents. The court members convict the accused as charged ('on divers occasions'), but—unknown to the parties or the military judge—in reality only convict the accused based upon two of the five incidents. On the surface, the court's finding matches the allegation—'on divers occasions.' Because the finding matches the allegation, it might initially appear that there are no *Walters* issues. But, the accused has, in reality, been acquitted of three separate incidents! . . . . More importantly, *Walters* is, at its core, grounded in the eventual concern that a military appellate court 'could not determine what conduct the accused had been found guilty of and what conduct he had been acquitted of.[18]

The concern is valid, but the courts have consistently held that in a divers occasions specification, the majority of the panel need only find the crime was committed more than once during the charged time frame. Because the members are simply agreeing in a general verdict that the elements have been met, they need not agree with each other as to which theories constitute guilt so long as at least two theories are supported by the evidence.[19] Therefore, an appellate court may be unable to determine, in a divers occasions case, those instances for which an accused was convicted *where the members were in agreement*; however, they also may be faced with a panel that convicted *based on different combinations and permutations* concluding in divers occasions being found by the majority. Both are valid results. Although troubling to some, the legality of this scenario has been routinely upheld by post-*Walters* decisions.

United States v. Rodriguez involved a divers occasions marijuana conviction.[20] Upon appeal, the appellant argued that "if the CCA found the evidence insufficient as to any of the uses undergirding the 'divers occasions' specification, [the] Court's decisions in Seider and *Walters* dictated that the entire specification be set aside."[21]

---

[18] Lieutenant Colonel John E. Hartsell & Major Bryan D. Watson, *The Decay of "Divers" and the Future of Charging "On Divers Occasions" In Light of United States v. Walters*, 61 A.F. L. Rev. 185, 191 (2008).

[19] Griffin v. United States, 502 U.S. 46, 46 (1991).

[20] United States v. Rodriguez, 66 M.J. 201, 201 (C.A.A.F. 2008).

[21] *Id*. at 203.

The Air Force Court of Criminal Appeals (AFCCA) found sufficient facts to convict on a singular count. The AFCCA distinguished *Seider* and *Walters* from *Rodriguez* because in the former, the *members* excepted the divers language, whereas in the latter, the Court of Criminal Appeals excepted it. As AFCCA explained, the members, as the factfinders returned a *general* conviction for marijuana use on divers occasions, thus enabling the court to find that any two or more of them could legally have been the basis of a conviction on divers occasions.

On review, CAAF agreed. At the outset, the Court concurred with the Appellant's contention that on a general finding of divers occasions, the appellate courts cannot specifically determine which instances formed the basis of the conviction. Even so, the Court nevertheless reaffirmed the "longstanding common law rule . . . that when the factfinder returns a guilty verdict on an indictment charging several acts, the verdict stands if the evidence is sufficient with respect to any one of the acts charged."[22] Interestingly, this was the same longstanding "'common law' rule on general jury verdicts" that was cited and disregarded as a basis to uphold the conviction in W*alters*.[23] The court in *Rodriquez* explains,

> When members find an accused guilty of an 'on divers occasions' specification, they need only determine that the accused committed two acts that satisfied the elements of the crime as charged, without specifying the acts, or how many acts, upon which the conviction was based.[24]

Further, the Court confirmed the presumption in a divers findings conviction that the verdict attaches to each of the several alternative theories and that a conviction can stand on appeal, despite trial errors, so long as any one occasion is deemed sufficient by the appellate court.[25] Moreover, the court noted that "the crux of [the *Walters* and *Seiders*] opinions was that the members' exceptions and substitutions on the findings worksheet implicitly meant that the factfinder had found that the accused was not guilty of some of the acts alleged at trial."[26] A general verdict does not. The Court made this point quite plain: "An unadulterated, unobjected-to, general verdict implicitly contains a verdict of guilt as to each underlying act and the CCA did not err in exercising its factual and legal review pursuant to Article 66, UCMJ here."[27]

More recently, the Navy provided additional insight on the general verdict issue.[28] *United States v. Fields* involved a request to alter the charge sheet from

---

[22] *Id*. at 204.

[23] United States v. Walters, 58 M.J. 391, 394 (C.A.A.F. 2004).

[24] *Rodriguez*, 66 M.J. at 203.

[25] *Id*. at 204 (quoting Griffin v. United States, 502 U.S. 46, 49 (1991)).

[26] *Id*. at 204.

[27] *Id*. at 205.

[28] United States v. Fields, No. 201100455, 2012 WL 1229443 (N.M. Ct. Crim. App. Apr 12, 2012)

a single act to divers occasions following arraignment. *Fields* was a larceny case involving a Navy PFC wrongfully using another member's check card to pay his own bills on four occasions. After both the Government and defense rested, the Government moved for a minor change to include "on divers occasions," or to draft the finding worksheet to allow the panel to choose one of the unauthorized purchases to satisfy the charge. Not surprisingly, the defense objected.[29] The military judge, while acknowledging that the case law is split, denied the Government request. The judge however, determined that defense had notice of all possible larcenies, and allowed the Government to offer four theories, from which the members could chose one to satisfy the single charge of larceny. The judge instructed the members that they could only convict on one of the four occasions.[30] On appeal, the Navy-Marine Corps Court of Criminal Appeals upheld the conviction.[31] No special findings were required.

United States v. Brown involved a single incident of indecent assault, which could have been satisfied on any of three alternate factual theories. While not a divers occasions case, its commentary is referenced in *Rodriguez* for its deference to panels who find guilt on differing bases. *Brown* held that "in federal criminal cases, the requirement for juror unanimity [majority in the case of courts-martial] applies only to elements of the offense."[32] In the military, the Court explains, "We have recognized that military criminal practice requires neither unanimous panel members, nor panel agreement on one theory of liability, as long as two-thirds of the panel members agree that the government has proven all the elements of the offense."[33]

As a general rule, therefore, the cases stand for the proposition that if the element of divers occasions is met, some members of the majority on review may

---

(denied review by CAAF. *See* 71 M.J. 380 (C.A.A.F. 2012)).

[29] *Id*.

[30] *Id.*

[31] *Id*. at *4.

[32] United States v. Brown, 65 M.J. 356, 359 (C.A.A.F. 2007). *Brown* is prefaced by a predecessor case from the Court of Military Appeals, *United States v. Vidal*. 23 M.J. 319 (C.M.A. 1987). In that case, an Army PFC was charged and convicted with rape. However, the facts did not specify whether he was the perpetrator or only held the victim down. The Court clarified, much like in Brown, "[u]nder such circumstances it has not heretofore been required that two-thirds of the members agree as to the particular theory of liability." The Court noted, by way of example:

> If one-third of the members are satisfied that the accused personally fired the shot and another third find that he aided someone else in doing so, he can properly be convicted of murder, because two-thirds of the court members are convinced beyond a reasonable doubt that the accused, on one theory or another, committed murder at the particular time and place.

Id.

[33] *Brown*, 65 M.J. at 359.

find it one way, some members another way, *et cetera*, with no impact on the legality of the conviction.

IV. PRACTICAL REASONS FOR CHARGING "ON DIVERS OCCASIONS"

A. Extensive Evidence Cases & Special Findings

In some cases, the government learns of the misconduct months after the criminal offense or offenses have allegedly taken place. Consequently, it becomes extremely difficult to go back in time and recreate with specificity exactly when an offense occurred and how many times it happened. This is especially true in cases involving multiple thefts over a lengthy period of time or multiple uses of illegal drugs over several months. Accordingly, prosecutors routinely and appropriately elect to enlarge the charged timeframe and charge the offense "on divers occasions" to allow them to encapsulate all of the alleged misconduct without tying their hands with a specific date. As the complexity of the crime increases and the length of time expands, this can make it more difficult for members and appellate courts to determine a single instance should it become necessary. In fact, some authors have voiced the following concern about divers charging following *Walters*:

> . . . the task of specifying misconduct with precision becomes exponentially more difficult as the number of criminal acts increases. Financial crimes, conspiratorial crimes, crimes of abuse over lengthy periods, and crimes involving hundreds of pieces of contraband, to name a few, may force the creation of an extensive findings worksheet with tailored exceptions and substitutions for each act and exhaustive lesser included offenses and potentially protracted instructions on how to vote on particular items which in the hands of lay court members may become a confounding agony of contradictions.[34]

While such a concern is valid, the process described takes place in courtrooms across the military all the time, typically resulting in just and valid outcomes. Moreover, there are still ways to mitigate the difficulty for members, counsel, and appellate courts.

First, in cases involving divers occasions, defense counsel can and should ask for a Bill of Particulars under Rule for Courts-Martial (hereinafter RCM) 906(b)(6), which requires detailed accounting of all elements of the allegations. Indeed, if the Government is not prepared to identify the specifics of every allegation, even if it requires "detailed lists of contraband," the charge is not legally sufficient, as required under RCM 906, such that it provides sufficient notice to the accused and

[34] Hartsell, *supra* note 18, at 190.

bars future prosecution. As it happens, this was brought up as a viable avenue for clarification of charges in the *Walters* dissent.[35]

Additionally, simplifying extensive collections of contraband or data is also frequently solved under Military Rule of Evidence (MRE) 1006. The vast majority of the documents introduced in the types of cases described in the above comment would otherwise fall under an exception to MRE 803, while MRE 1006 enables the use of summaries, which may be "presented in the form of a chart, summary, or calculation."[36] Using MRE 1006 provides significant leeway for the Government to alleviate the "agony" of our military panels.

Finally, the military judge can and should modify the findings instructions to account for variables raised by the evidence in the case. For example, suppose a thief had stolen a hundred items, all of differing character, from different locations, at different times, and charged as larceny of military property over $500 on divers occasions. This might appear to pose an issue where the appellate court could not ascertain which items the members identified as satisfying the crime without a hundred-item special findings worksheet. However, if the findings made are a general verdict, then the appellate court would only have to determine that there were at least two occasions of stealing military property worth over $500 to uphold the conviction. Moreover, even if the members excepted the words "on divers occasions," the military judge would simply need to instruct the members that a majority of them must agree upon a specific instance and that the item(s) taken on specific occasion were of a value greater than $500. Providing a few lines for the members to describe the instance or the items taken on a particular occasion would be sufficient to withstand a *Walters* review.

All of these approaches make sense when one considers the underlying holding of *Walters*. The extent of the holding, as the court explained, applies only in those "narrow circumstance[s] involving the conversion of a 'divers occasions' specification to a 'one occasion' specification through exceptions and substitutions," by the panel members.[37] Whether or not the court realized the potential philosophical quagmire that could be drawn from the theory of their ruling remains to be seen. However, subsequent case law has seen fit to keep this case narrow, or else distance itself from the ruling.

B. Post-Walters Sentencing

Another issue raised post-W*alters* is that following a general conviction on divers occasions, "[t]he subsequent sentencing case by the parties may have no resemblance to the conviction actually handed down by the members."[38] Indeed,

[35] United States v. Walters, 58 M.J. 391, 397-398 (C.A.A.F. 2003).

[36] MCM, *supra* note 2, Mil. R. Evid. 1006.

[37] *Walters*, 58 M.J. at 396.

[38] Hartsell, *supra* note 18 at 191.

if there are no special findings required in a conviction on divers occasions, how can an argument be made in aggravation, or mitigation, without knowing of what the individual was actually convicted?

To answer this question, we should consider the common uses for charging on divers occasions. One common example is wrongful use of drugs over a period of time. Routinely, this results from a failed urinalysis test, followed by a failed *Bickel* test.[39] There is frequently no substantive question of fact such that members would question the underlying charge or come to conflicting determinations as to the basis of conviction. Another common scenario is a failed urinalysis followed by a confession to additional uses of drugs. Then the question becomes whether the ultimate sentence should be substantially different if the member used the drug two times or five times. The final scenario worth consideration is the case of a single urinalysis test accompanied by witness testimony of additional misconduct from other drug abusers, or worse, a case *entirely* supported by "dirty" witness testimony. Insofar as there is a question as to the legitimacy of any one of the instances of misconduct, the use of divers would be misapplied anyway, in favor of individual specifications for each instance.

However, there is a solution to concerns over appropriate sentencing arguments in cases of "divers occasions," where the number of occasions the members convicted on is unclear. *Vidal, Brown*, and *Fields* provide insight. Indeed, the core of these cases is that the Government may prove a single charge on alternate theories of liability. In *Vidal*, this was through the alternate theories of perpetrator versus aider and abettor. In *Brown*, the alternate theories related to the multiple methods for proving indecent assault, the lesser included offense of the charged rape. *Fields* involved proving one charge through any of several related instances of larceny.

These admittedly did not involve divers occasions. However, alternate theories could be equally as applicable to divers occasions as to single specifications with multiple methods of liability. In a case involving several *known* instances of misconduct charged as divers, a conviction on two or more, but less than all of the alleged instances, could result in a sentencing case using the alternative theories argument. In other words, following a conviction for larceny on divers occasions, the Government could conceivably argue each larceny as warranting graduating sentence results depending on the basis of their conviction. For example, each larceny is worth ten days in jail or anything greater than two warrants a bad conduct discharge. Prosecutors are frequently encouraged to assign numbers to punishments in order to guide the members without telling them, carte blanche, how to rule. In many ways, this empowers the members. Furthermore, there is no reason to think that a similar approach in a divers occasions case in which the number of infractions

[39] United States v. Bickel, 30 M.J. 277 (C.M.A. 1990) (upholding follow-on inspection urinalysis after failed urinalysis test).

is *unknown* would not be equally effective. Where there is a real question over the number of instances the members deemed met the elements, a possible way of handling it is to simply argue generally that the crime was committed more than once, and then articulate why having done the crime on more than one occasion justifies the increased punishment. While this may not be ideal in all cases, it offers a reasonable stop-gap measure.

V. CONCLUSION

As this article has demonstrated, the actual fall-out from *Walters* has been negligible. Although there remain cases that occasionally get overturned because special findings are not properly required by trial judges in *Walters*-like scenarios, those cases are the exception and not the rule. Additionally, in the ten years since *Walters*, the appellate courts have not expanded the holding. In fact, general verdicts in "divers occasions" cases continue to be upheld on appeal and the courts have expressed no concerns about using their fact-finding powers to determine whether or not the facts support at least two occasions. Consequently, the use of "divers occasions" remains a valid means of charging cases in which there is a continuous course of criminal conduct and the government is unable to easily ascertain the facts with sufficient specificity to break it out into separate specifications. Although there remains some concern about the ambiguity in general verdicts when it comes to sentencing, there are several viable argument methods to overcome this obstacle. Prosecutors should not therefore shy away from charging offenses on divers occasions. They should, however, be aware of the ramifications of doing so. Then, and only then, may a prosecutor be certain that the proposed approach is the appropriate one.

HIGH (RISK) SOCIETY: EASING THE ANXIETY FOR INSTITUTIONAL CLIENTS USING SOCIAL MEDIA

Susan L. Turley[*]

[*] The views expressed are those of the author and do not represent the official views of the Department of Defense, the Air Force, the Army, or any of their organizations. Lieutenant Colonel (retired) Susan L. Turley (B.A., with high honors, University of Arizona (1983); J.D., with high honors, University of Texas (1995); LL.M., distinguished honor graduate, The Judge Advocate General's School of the Army, Charlottesville, Virginia (2002)) is the contract and fiscal law attorney with the Office of the Staff Judge Advocate, Army Network Enterprise Technology Command, Fort Huachuca, Arizona. Before her current position, she served as an acquisition attorney in the Legal Information Services directorate of the Air Force Legal Operations Agency, Maxwell Air Force Base, Alabama; and as the Deputy Staff Judge Advocate at Air University at Maxwell. She is a member of the bars of Alabama and Texas.

A police officer describes his job to friends as "human waste disposal." He's placed on desk duty while his department investigates.[1] *Who made the mistake—the department or the officer?*

A federal government employee, confused about the advice her agency lawyer has provided, discusses it with others in her field—all outside her agency.[2] *Has she waived privilege?*

A citizen tries to inform a government agency of a life-threatening situation, but the agency never processes and acts on the information. Is the agency negligent?[3]

Now add in the factor that each scenario deals with some form of social media, including Facebook, Twitter, chat rooms and blogs. Does that matter? Should it?

I. INTRODUCTION

This article asserts that lawyers' ability to help their clients understand the third- and fourth-order consequences (and sometimes beyond) is becoming increasingly critical when dealing with technology in all its forms but especially social media. The use of social media has reached near-total saturation both among private citizens and U.S. Government agencies. According to some statistics, more than two-thirds of adults online use social media,[4] while as of 2012, "every major federal agency" was using Twitter and YouTube, and all but one had a Facebook presence.[5]

---

[1] Erica Goode, *Police Lesson: Social Network Tools Have Two Edges*, N.Y. Times, Apr. 7, 2011, at A1, *available at* http://www.nytimes.com/2011/04/07/us/07police.html?pagewanted=all&_r=0.

[2] *See Contract Award Process: Posting, Synopsis, and Advertisement*, Wifcon Forum And Blogs (Jun. 22, 2009), 8:58 a.m.), http://www.wifcon.com/discussion/index.php?showtopic=240 (federal employee soliciting input through online forum regarding information previously discussed with agency attorney).

[3] *See* Joseph Marks, *Social Media Brings New Capacities and Liabilities to Crises*, NextGov.com (Aug. 31, 2011), http://www.nextgov.com/technology-news/2011/08/social-media-brings-new-capacities-and-liabilities-to-crises/49704/ (discussing potential civil liability of emergency responders for failure to routinely monitor social networking sites for incident reports).

[4] Joanna Brenner, *Pew Internet: Social Networking*, Pew Res. Ctr (Nov. 13, 2012), http://pewinternet.org/Commentary/2012/March/Pew-Internet-Social-Networking-full-detail.aspx. According to the research on social networking, 63 percent of men and 75 percent of women who use the Internet also use social networking sites. For those between the ages of eighteen and twenty-nine, the figure is a staggering but not surprising 92 percent. Facebook is the overwhelming medium of choice, used by 66 percent of adults online. *Id*.

[5] Joseph Marks, *All Major Federal Agencies Now Using Twitter and YouTube*, NextGov.com (Apr. 9 2012), http://www.nextgov.com/cio-briefing/2012/04/all-major-federal-agencies-now-using-twitter-and-youtube/50991/.

Given this societal infiltration, attorneys and clients should not ignore social media, and they cannot rely on traditional sources such as legislatures and the courts for guidance:

> The judiciary risks error by elaborating too fully on . . . implications of emerging technology before its role in society has become clear. . . . Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior. . . . [T]he law is beginning to respond to these developments . . . [but] it is uncertain how workplace norms, and the law's treatment of them, will evolve. [6]

Thus, clients will expect their attorneys to help them navigate through cyberspace.[7] This article attempts to give lawyers some tools for doing so by focusing on a few key factors in analyzing social media actions. In this context, "social media" means any form of real-time, interactive communications, including Facebook, Twitter, LinkedIn, blogs, chat-rooms, and instant messaging (IM).[8] This article assumes a basic understanding of how each application works, which should be enough in most cases.[9]

II. ATTORNEYS AS MYTHBUSTERS

Albert Einstein once said, "Only two things are infinite, the universe and human stupidity, and I'm not sure about the former."[10] The 21st-century corollary to that axiom is that nothing is more infinite than human stupidity posted online.[11]

---

[6] City of Ontario, Cal. v. Quon. 130 S. Ct. 2619, 2629-30 (2010) (internal citations omitted). *But see id*. at 2635 (Scalia, J., concurring) ("The-times-they-are-a-changin' is a feeble excuse for disregard of duty.").

[7] The American Bar Association's Commission on Ethics 20/20 has recommended that the Model Rules of Professional Conduct make technological knowledge a basic requirement for maintaining competence. The proposed Comment to Rule 1.1 reads: "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology . . . ." Jamie S. Gorelick and Michael Traynor, *Report to the House of Delegates*, A.B.A. Comm'n on Ethics 20/20 Rep. 2 (2012) (emphasis in original to indicate proposed new language), *available at* http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/2012_hod_annual_meeting_105a_filed_may_2012.pdf-25k-2012-08-09.

[8] Linda D. Schwartz, *Social Media—Friend or Foe*, Md. B. J., Mar.-Apr. 2011, at 13, 13-14.

[9] See *id*. for a succinct discussion of how each program works and the differences between them.

[10] Albert Einstein, BrainyQuote.com, http://www.brainyquote.com/quotes/quotes/a/alberteins100015.html, (last visited Feb. 7, 2013).

[11] "Driven by a 'self-destructive combination of ignorance, narcissism, and generation-specific disregard for their own privacy,' Facebook-posting crooks are making life much easier for cops." *Seven Suspected Criminals Who Got Themselves Caught Via Facebook*, The Wk., Apr. 26, 2012 (quoting Winston Ross of *The Daily Beast*), http://theweek.com/article/index/227257/7-suspected-criminals-who-got-themselves-caught-via-facebook.

Not only is it infinite, it is undying and ubiquitous. [12] It is *not*, however, anonymous, exclusive, retractable or containable. At times it is reliable, and at times it is not. Similarly, it sometimes enjoys the protection of the First Amendment, copyright laws, privilege or other legal safeguards, but sometimes it may also impose significant liability or destroy any safety nets the law offers. Thus, one of the most fundamental tasks an attorney may perform is helping the client understand the realities of any social media foray.[13]

Early on, attorneys and clients should determine where the social media use falls on the following scale:

- Intended to be entirely internal: Twitter or IM sent only to organizational addresses, chat rooms open only to organizational members, or private social networking site pages;
- Internal to external: Postings by organizational members on public Facebook (or similar site) pages, company blogs, or Twitter messages ("tweets") to all followers; or,
- External to internal: Communications to or about the client from external sources, for example, postings by non-members of the organization to a Facebook page, comments to a blog, or tweets about a company.

III. PRIVACY? WHAT PRIVACY?

For all social media but especially for those communications intended to be entirely internal, the initial reality check is to help the client understand that privacy and restricted use or dissemination often disappear in cyberspace. Arguably, only secure, properly labeled, and selectively distributed e-mails carry any privacy protections,[14] and as WikiLeaks demonstrated, the integrity of those protections

[12] *See* Jeffrey Rosen, *The Web Means the End of Forgetting*, N.Y. Times Sun. Mag., Jul. 25, 2010, at MM32, *available at* http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?pagewanted=all (discussing the "permanent memory bank of the Web").

[13] This article does not attempt to address the issues involved when attorneys—not their clients—use social media, although the two areas do overlap. For attorney-specific guidance, see generally Steven C. Bennett, *Ethics of Lawyer Social Networking*, 73 Alb. L. Rev. 113 (2009); David J. Lender & Keith Gibson, *Ethics in an Electronic World*, 8 Litig. & Admin. Prac. Course Handbook Series 419, Practising L. Inst. (2008); David G. Ries, *Cyber Security for Attorneys: Understanding the Ethical Obligations*, L. Prac. Today (Mar. 2012), http://www.americanbar.org/content/dam/aba/publications/law_practice_today/cyber-security-for-attorneys-understanding-the-ethical-obligations.pdf-8k-2012-03-16; Gretchen M. Nelson, *Practicing Law Ethically in a Changing Technological World*, 25 ABA Spg. Brief 32 (2006); David Hricik et al., *Ethics and the Internet*, 57 Prac. Law. 21 (2011).

[14] *See generally* Louise L. Hill, *Gone but Not Forgotten: When Privacy, Policy and Privilege Collide*, 9 Nw. J. Tech. & Intell. Prop. 565 (2011) (discussing privacy and privilege expectations for workplace communications).

depends on the integrity of the receiver. [15] When using a social media site, "private" is a relative term.[16]

In 2012, the U.S. Marine Corps discharged Sergeant Gary Stein because of comments he posted online, making Stein a "public example of how the Marines handle personal opinion in the Internet age."[17] Stein co-founded the Armed Forces Tea Party website, knowing that "he had to tread a fine line as an active-duty Marine, with legal limits on public political activity." [18] Those limits are set by Department of Defense Directive (DoDD) 1344.10, *Political Activities by Members of the Armed Forces*, which prohibits active-duty military members from engaging in most "partisan political activity" (other than voting).[19] This includes publishing "partisan political articles, letters, or endorsements signed or written by the member that solicit votes for or against a partisan political party, candidate, or cause" and participating "in any radio, television, or other program or group discussion as an advocate for or against a partisan political party, candidate, or cause."[20]

Among other things, Stein said on Facebook, "As an active-duty Marine, I say, 'Screw Obama,' and I will not follow the orders from him—all orders from him."[21] Although acknowledging that his comments were "not tasteful," Stein and his attorneys claimed that the First Amendment still protected his online speech.[22] The Marine Corps disagreed and discharged Stein with a "less than honorable" characterization of service.[23]

While DoD policies on personal freedom of expression may be more restrictive than most organizations, the military is certainly not alone in monitoring internal communications and using them for disciplinary actions. In April 2011, the

---

[15] *See* Malcolm Rifkind, *WikiLeaks: Do They Have a Right to Privacy?*, Telegraph Blog (London) (Nov. 30, 2010, 7:12 a.m.), http://www.telegraph.co.uk/news/worldnews/wikileaks/8169712/WikiLeaks-Do-they-have-a-right-to-privacy.html (noting that the 250,000 confidential U.S. State Department messages revealed by WikiLeaks were stored on "a Pentagon-run electronic database that could be accessed, quite properly, by at least tens of thousands and, possibly, hundreds of thousands of officials and military personnel with the appropriate security clearance").

[16] *See* Hricik et al., *supra* note 11, at 33 (asserting that while social networking sites "on their face seem 'private' to some extent . . . . there is a significant amount of information available" to anyone who wants to look).

[17] Brian Rooney, *Sgt. Gary Stein, Discharged for Obama Criticism, "Scared," Not Backing Down*, CBS News (May 4, 2012), http://www.cbsnews.com/8301-505263_162-57427802/sgt-gary-stein-discharged-for-obama-criticism-scared-not-backing-down/.

[18] *Id.*

[19] U.S. Dep't. of Def. Directive 1344.10, Political Activities by Members of the Armed Forces, para. 4 (19 Feb. 2008) [hereinafter DoDD 1344.10].

[20] *Id*., paras. 4.1.3.2, 4.1.2.6.

[21] Rooney, *supra* note 17.

[22] *Id*.

[23] *Id*. See *infra* notes 167-180 and accompanying text for a discussion of the legal issues surrounding Stein's discharge.

National Labor Relations Board (NLRB) accused Thomson Reuters, parent company of Westlaw, of illegally disciplining an employee who sent a Twitter message to a *company* address in response to a *company* request for input on improving working conditions.[24] A supervisor at the Reuters news division had encouraged workers to post messages on "how to make Reuters the best place to work."[25] In response, the employee, who was a reporter and also head of the Newspaper Guild at Reuters, tweeted, "One way to make this the best place to work is to deal honestly with Guild members."[26] The next day, the employee said, her bureau chief called her at home and reprimanded her for violating a policy against damaging the company's reputation. [27]

While both these scenarios involved adverse actions against individuals who may have thought their social media musings were protected, clients must assume that all social media information can and probably will be compromised. One federal office charged with "operations security" (OPSEC) cautions that social media security for the most part is an illusion.[28] Whether through negligence or malfeasance, cunning or luck, inadvertently or deliberately, someone somewhere will probably breach the best of safeguards—and may even do so legally.

In 2010, a California county bought some software from a commercial developer, loaded it on the county's servers, and then gave its password to a competing software company, allowing the competitor to access the program and obtain the software source code.[29] The court ruled that the county had committed no civil or criminal fraud.[30] Skype has become one of the world's most popular video chat tools, partly because it was thought to be safe from wiretapping.[31] Then, in early 2011, "after storming the secret police headquarters, Egyptian activists

---

[24] Steven Greenhouse, *Labor Panel to Press Reuters Over Reaction to Twitter Post*, N.Y. Times, Apr. 7, 2011, at B3.

[25] *Id*.

[26] *Id*.

[27] *Id*.

[28] *See OPSEC and Social Networking*, Interagency OPSEC Support Staff [hereinafter IOSS], at slide 26 (undated PowerPoint training slides) (on file with author) (warning that the lack of security cannot be overemphasized). The IOSS, established in 1988, is a federal agency run by the National Security Agency that helps other U.S. government organizations create and maintain robust agency OPSEC programs. "OPSEC" refers to methods designed to "identify, control, and protect unclassified information and evidence associated with U.S. national security programs and activities." *About the IOSS*, Nat'l OPSEC Program, https://www.iad.gov/ioss/department/about-the-ioss-10019.cfm?killnav=1 (restricted access website) (last visited Feb. 4, 2013).

[29] *Atpac v. Aptitude Solutions*, 730 F. Supp. 2d 1174 (E.D. Cal. 2010).

[30] *See id*. at 11832-83 (holding that "the simple . . . and… very common act of giving someone else your password . . . is not a crime…").

[31] *See Skype Could Force End to Wiretapping Calls*, Associated Press, Feb. 16, 2006, *available at* http://www.msnbc.msn.com/id/11393674/ns/technology_and_science-security/t/skype-could-force-end-wiretapping-calls/ (reporting that Skype, the fastest growing Internet calling service, was the only such service to offer encrypted calls, making them potentially "impossible to snoop on").

discovered that the Mubarak government had been using a trial version of a tool—developed by Britain's Gamma International—that allowed them to eavesdrop on Skype conversations."[32]

Here in the United States, the federal government warns as well that U.S. users should not assume that their social media postings remain in the country and are thus covered by domestic data protection laws. "How many different companies and services are involved in providing the . . . service? What if the owners are foreign . . . does their hosting service reside in a foreign country? . . . If you don't consider these factors, you are handing your data over" to outsiders who may have only their own best interests at heart.[33]

Finally, social media, regardless of the perceived privacy, falls into the category of potentially discoverable evidence—and as with all other electronically stored information, "deleted" does not mean gone.

> Twitter saves all users' tweets, and last year, the Library of Congress acquired the entire public Twitter archive; Facebook pages are maintained until the user deletes or overwrites them; Google+ data is similarly stored . . . . [I]n the fine print of Terms of Service, users are not ensured a right to privacy for anything posted on a third-party, semi-public, "free" social media platform. And as case law around social media develops, users' privacy will further dissolve as more social media platform providers are forced to hand data over to the courts.[34]

The question is not *if* a client will be asked to turn over social media, the question is *when*.[35] Consequently, a lawyer must advise clients to assume that someone will read their social media communications: "No matter what, things you post might spread. If you're not comfortable with it being public knowledge, don't post it."[36]

---

[32] Evgeny Morozov, *Political Repression* 2.0, N.Y. Times, Sept. 2, 2011, at A23. However, even those who normally do the snooping or surveillance are not immune from incursions. The U.S. Government's international broadcasting agency provides sophisticated technology to residents of "high-censorship nations" to enable them to circumvent state-imposed Internet blocks. These tools conceal the identities and viewing habits of online users and prevent the act of viewing a site from triggering a government attempt to shut it down. Joseph Marks, *Agency Uses Circumvention Tools to Advance Democracy*, NextGov.com (Aug. 23, 2011), http://www.nextgov.com/technology-news/2011/08/agency-uses-circumvention-tools-to-advance-democracy/49648/.

[33] IOSS, *supra* note 28, at slide 10.

[34] Joshua Kubicki, *From the Experts: Read the Fine Print Before You Tweet*, Law.com, Sept. 23, 2011, http://www.law.com/jsp/cc/PubArticleCC.jsp?id=1202516485525

[35] *Id*. (reporting that one study predicts that more than half of all companies will be hit with discovery requests for social media evidence by the end of 2013).

[36] IOSS, s*upra* note 28, at slide 26.

IV. DIDN'T YOU GET MY MESSAGE?

Now turn the circumstances around: Instead of the wrong people seeing the wrong information, the right people do not see the right information—a scenario that can also generate legal headaches. Tammy Blakey was Continental Airlines' first female captain to fly the Airbus 300, a wide-body twin-engine jet.[37] During the 1990s, Blakey sued Continental, claiming, among other things, that she had been sexually harassed by messages posted on the pilots' online computer bulletin board.[38]

A commercial provider, CompuServe, provided Internet access to the Continental "Crew Management System" (CMS), which contained information on crew member schedules, flights, pairings and pay.[39] Only identified Continental crew members could access the CMS. As part of its contract with Continental, CompuServe also offered a Crew Member Forum as an electronic way for users to exchange information and opinions.[40] Continental managers supposedly were not allowed to use the Forum, and no one in company management monitored or reviewed the postings. However, chief pilots and assistant chief pilots—considered part of Continental "management"—could log into the Forum. Additionally, other crew members voluntarily provided technical support and troubleshooting services and policed Forum usage.[41]

After Blakey filed a federal discrimination claim against Continental, she became the subject of Forum postings by co-employees that she considered defamatory and sexual harassment. She then brought a civil case that was tried in New Jersey state court. Both the trial and appellate courts ruled that the Forum did not constitute a "workplace for purposes of a hostile work environment."[42] However, the New Jersey Supreme Court reversed and remanded the case, holding that communications purely online and outside the workplace could create a hostile work environment.

> Although the electronic bulletin board may not have a physical location within a terminal, hangar or aircraft, it may nonetheless have been so closely related to the workplace environment and beneficial to Continental that a continuation of harassment on the forum should be regarded as part of the workplace. . . . Thus, standing alone, the fact that the electronic bulletin board may be

[37] Blakey v. Continental Airlines, 751 A.2d 538, 543 (N.J. Sup. Ct. 2000) (reversing the lower court's decision).

[38] *Id*.

[39] Blakey v. Continental Airlines, 730 A.2d 854, 857-58 (N.J. Sup. Ct. 1999).

[40] *Id*. at 858.

[41] *Id*. at 858-59.

[42] *Id*. at 860.

> located outside of the workplace . . . does not mean that an employer may have no duty to correct off-site harassment by co-employees.[43]

Consequently, employers may be accountable for conditions arising from workers' social media usage, even if the communications are "unofficial" and entirely among company personnel. But if organizations become too oppressive or repressive in their social media policies and monitoring, they may find themselves called on the virtual carpet, as Reuters did in the case described earlier.[44] Reuters was not alone: for the first time ever, in 2011, the NLRB's Office of the General Counsel issued a report on social media cases (a total of 14) from the previous year.[45]

While it may not create the foundation for a hostile work environment, information that flows from outside the organization may still degrade performance or cause legal difficulties if the right people do not receive and process it. For institutional clients that solicit feedback but then do not respond to it, the result may be a customer who not only was disgruntled enough to complain initially but is now even unhappier that he has been ignored.[46] Although not necessarily a legal problem *per se*, dissatisfied customers do not usually bode well for the client—nor thus for the attorney. However, if the organization has some obligation to act on the information, the legal implications could be far more serious.

Numerous U.S. Government agencies have woven social media tools into their emergency-preparedness and disaster-response plans, including the Federal Emergency Management Agency (FEMA), the Department of Homeland Security (DHS), the Federal Communications Commission (FCC),[47] the National Weather Service, the National Oceanic and Atmospheric Administration (NOAA) and the National Aeronautics and Space Administration (NASA).[48] For example, in 2011, FEMA and the FCC launched the Personal Local Alert Network (PLAN), which will send location-based alerts regarding "imminent threats" to mobile devices.[49] The system, which comes at no cost to consumers, uses broadcast technology

---

[43] Blakey v. Continental Airlines, 751 A.2d 538, 543, 549 (N.J. Sup. Ct. 2000).

[44] *See* Greenhouse *supra* notes 24-27 and accompanying text; *see also infra* notes 89-120 (discussing social media policies).

[45] Nat'l Lab. Rel. Board, *Report of the Acting General Counsel Concerning Social Media Cases*, Aug. 18, 2011[hereinafter NLRB 2011], *available at* http://nlrb.gov/news/acting-general-counsel-releases-report-social-media-cases.

[46] Roger Dooley, *Why Ignoring Social Media Complaints is a Huge Mistake*, Forbes CMO Network (Sep. 18, 2012, 8:05 AM), http://www.forbes.com/sites/rogerdooley/2012/09/18/complaints/.

[47] Erin Skarda, *How Social Media Is Changing Disaster Response*, Time (Jun. 9, 2011), http://www.time.com/time/nationa/article/0,8599m2966195,00.html.

[48] Brandon Griggs, T*witter Accounts for Storm, Relief Updates*, CNN.com (Oct. 29, 2012), http://www.cnn.com/2012/10/29/tech/social-media/storm-sandy-social-media.

[49] Damon Penn, *Emergency Alerts Delivered to Your Phone: What Our New PLAN Means to You*, FEMA Blog (May. 13, 2011, 6 PM), http://blog.fema.gov/2011/05/emergency-alerts-delivered-to-your.html.

that supposedly will ensure "alerts will get through even if cellular networks are swamped."[50] During Hurricane Sandy in 2012, the National Weather Service, NOAA and NASA tweeted satellite images of the storm, weather and flooding forecasts, and analyses, while FEMA sent out safety tips and information on shelters.[51]

As more organizations leverage social media, they must remember that most people in their audience expect social media to be a two-way street—that is, if they *receive* information through social media, they also expect to be able to *deliver* it that way. This becomes especially critical in a disaster, when the Internet may be the only form of communication network available.[52] A 2010 Red Cross survey found that more than a third of those surveyed would use an agency's Facebook page to send a direct request for emergency assistance, while more than a fourth would use Twitter—"and they expect first responders to be listening."[53] Sixty-nine percent of survey participants said "emergency responders should be monitoring social media sites in order to quickly send help," and "74 percent expected help to come less than an hour after their tweet or Facebook post."[54] A year later, the number of people who expected disaster-response agencies to monitor social media was up to 80 percent.[55] Those first responders who leverage social media as a way to communicate with the public but then fail to keep an eye on that media potentially expose themselves to liability.

> As a general rule, federal emergency responders are legally required to act only on information citizens should reasonably expect that they've received . . . . Five years ago, few people would have expected a local fire department to be constantly checking its Facebook page, but as social media surges in popularity, those presumptions may change . . . and the fire station's liability along with them. [56]

What if the intended recipient does receive and read the information, but it turns out to be inaccurate? During 2012's Hurricane Sandy, a Twitter user with the handle "Comfortably Smug" dispatched a plethora of tweets about the storm's

---

[50] *Id.*

[51] Griggs, *supra* note 48.

[52] *See* Skarda, *supra* note 47 (noting that while "conventional telephone lines often go down or become overwhelmed during a disaster, Internet connections often remain active and usable").

[53] Press Release, Web Users Increasingly Rely on Social Media to Seek Help in a Disaster (Aug. 9, 2010), *available at* http://newsroom.redcross.org/2010/08/09/press-release-web-users-increasingly-rely-on-social-media-to-seek-help-in-a-disaster/.

[54] *Id.*

[55] Wendy Harman, *How Social Media is Shaping Disaster Response,* ForbesBrandVoice (Mar. 17, 2012, 2:31 PM), http://www.forbes.com/sites/dell/2012/03/07/how-social-media-is-shaping-disaster-response/.

[56] Marks, *supra* note 3 (quoting Philadelphia attorney Edward Robson).

damages, including claims that three feet of water covered the floor of the New York Stock Exchange and that Manhattan was going to lose all electricity.[57] The National Weather Service website, along with CNN news reports and 500 other Twitter users, spread the Wall Street flood report before it was disproven.[58] One local official compared the tweets to the "digital equivalent of showing 'Fire' in a crowded theater."[59]

For years, the U.S. Geological Survey (USGS) has run an "earthquake report crowdsourcing page" called "Did You Feel It?" (DYFI?)[60] Within hours of the massive earthquake that rattled the East Coast on August 23, 2011, the site collected a record 140,000 responses, with reports flowing in at a rate of about 13 per second at one point.[61] The agency developed the site to help improve government understanding of earthquakes, and apparently it works. USGS researchers are able to use citizen reports to quickly generate damage assessments that would otherwise take weeks. One researcher "has been able to pinpoint the epicenter of an earthquake within seconds based on the origin of a spike in Tweets using the word 'earthquake'."[62]

The USGS says the "site has been largely free of pranksters . . . so geologists have to do very little sifting out of false reports."[63] Imagine, however, that relief agencies acted quickly on these extrapolated, citizen-based damage assessments; those assessments were later shown to be flawed; and, as a result, the earthquake losses were greater than they should have been. As one mapping-industry official pointed out, a Twitter search for a named hurricane could return all sorts of interesting but not necessarily useful results.[64]

Social media's near-instantaneous transmission speed magnifies both the likelihood and the impact of misinformation. While experts can hopefully distinguish between relevant and irrelevant data, in a disaster's chaotic, rushed first moments when timely, on-target responses are most crucial, bad information could itself wreak additional havoc, both for emergency response teams and victims themselves.[65] To

---

[57] Doug Gross, *Man Faces Fallout for Spreading False Sandy Reports on Twitter*, CNN.COM, Oct. 31, 2012, http://www.cnn.com/2012/10/31/tech/social-media/sandy-twitter-hoax.

[58] *Id*.

[59] *Id.*

[60] Joseph Marks, *Mineral, Va., quake?: "Yea, we felt it."* NEXTGOV.COM (Sept. 28, 2011), http://www.nextgov.com/technology-news/2011/09/mineral-va-quake-yeah-we-felt-it/49851/.

[61] *Id*.

[62] *Id*.

[63] *Id*.

[64] Marks, *supra* note 3. A Google search for "hurricane" and "Lola" brought back 4.49 million results, including photographs of a "floofy-tailed" cat of the same name, an offer to find "Lola Lively" in Hurricane, W.V., and a YouTube video of would-be star Lola Banks urging viewers to "forget making it rain, make it hurricane." Google search conducted Sept. 30, 2011 (results on file with author).

[65] *See* Marks, *supra* note 3 (asserting that inaccurate information could "divert responders . . . and

avoid exacerbating any crisis, agencies must not only monitor citizen social-media input but they must winnow out the inaccuracies and fine-tune their response—all within minutes.[66]

V. WIDE OPEN (CYBER)SPACES?

Perhaps because of the absence of physical boundaries, some users view cyberspace as similarly lacking legal restrictions, subscribing to the "widely held belief that the Internet is a legal no man's land, where people are free to publish what they wish without fear of censure or repercussions."[67] Some of this attitude may flow from the myths of privacy and protection discussed earlier, but some of it may also spring from the belief that information found online is free for the taking—and the using. Depending on the circumstances, the result could be ethically questionable plagiarism or legally dangerous copyright infringement, and the risk is growing: "[A]s concepts of intellectual property, copyright and originality are under assault in the unbridled exchange of online information. . . . The Internet may be redefining how [users] . . . understand the concept of authorship and the singularity of any text or image."[68]

Simply because an online posting does not have an obvious, individual author or because the information is widely available does not mean it can be used with impunity. Copyright laws affect virtual intellectual property just as they do hard-copy works.[69] The *New York Times*, for example, tells users that online stories are meant for "personal, noncommercial use" only.[70] Is reposting a link to a Facebook page a "personal, noncommercial use?" Is that Facebook page a "personal, noncommercial" page? If it is not—that is, it is an organizational Facebook page—then posting the link is similarly not a personal, noncommercial use. Admittedly, under most circumstances, the *New York Times* will not complain that the client has provided additional publicity, assuming that the client gives credit where credit is

---

potentially create liability issues"); Skarda, *supra* note 47 ("Of course, as with anything on the Web, social media has a tendency to breed rumors and inaccuracies that could hurt recovery efforts.")

[66] *See* Harman, *supra* note 55 ("Those of us in the emergency management and relief sector have had to adjust to monitor the public's reports and response more efficiently.")

[67] David Ardia, *Bloggers and Other Online Publishers Face Increasing Legal Threats*, Poynter Online, Sep. 22, 2008, 11:19 a.m., *available at* http://www.poynter.org/latest-news/top-stories/91639/bloggers-and-other-online-publishers-face-increasing-legal-threats/.

[68] Trip Gabriel, *Plagiarism Lines Blur for Students in Digital Age*, N.Y. Times, Aug. 1, 2010, at A1, *available at* http://www.nytimes.com/2010/08/02/education/02cheat.html?pagewanted=all&_r=0. The article describes a student who copied from Wikipedia but "thought its entries—unsigned and collectively written—did not need to be credited since they counted, essentially, as common knowledge." *Id*.

[69] Ardia, *supra* note 67.

[70] N.Y. Times, *Terms of Service*, http://www.nytimes.com/content/help/rights/terms/terms-of-service.html (last visited Feb. 6, 2013).

due. However, the newspaper may not be so understanding if the client publishes passages lifted wholesale from the publication on a commercial blog.[71]

In some cases, the "fair use" exception in copyright law protects using copyrighted work "for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research" based on the following factors:

> (1) the purpose and character of the use, including whether such use is of a commercial
> (2) nature or is for nonprofit educational purposes;
> (3) the nature of the copyrighted work;
> (4) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
> (5) the effect of the use upon the potential market for or value of the copyrighted work.[72]

Deciding, however, whether a social media communication falls under the fair-use exception requires some effort and depends heavily on the specific facts and circumstances.[73] For purely commercial activities, the safest course of action will be to obtain the copyright holder's permission.

While copyright infringement may be the most obvious legal risk for social media postings, it is not the only one. In today's environment, where setting up a blog requires no real technical expertise,[74] even institutional clients may not possess the electronic sophistication to understand the consequences of their postings. Most social media users recognize that posting something false could open them up to defamation claims,[75] but they may not realize that disseminating truthful information may also trigger liability. Truth may be no defense, and good intentions may not help either.

---

[71] *See* Ardia, *supra* note 63 (noting that copyright infringement claims have increased against "celebrity-gossip bloggers").

[72] 17 U.S.C. §107 (2010).

[73] *See* Jeffrey D. Neuburger, *New Media, Technology and the Law: A Summary of Key Legal Developments Affecting Technology and Emerging Business Models*, at 195, 202 (PLI Intell. Prop. Course Handbook, Course Handbook Ser. No. G-1034, 2011) (warning that such determinations "involve an extremely fact-sensitive consideration of the non-exclusive, statutory fair use factors under 17 U.S.C. §107").

[74] *See* Martin LaMonica, *The Do-it-Yourself Web Emerges*, CNET News, Jul. 31, 2006, http://news.cnet.com/The-do-it-yourself-Web-emerges/2100-1032_3-6099965.html#ixzz1ZYo0OGIb (reporting on the proliferation of web sites intended to "empower non-programmers" to create their own sites).

[75] For an in-depth discussion of electronic defamation principles, *see* David S. Ardia, *Reputation in a Networked World: Revisiting the Social Foundations of Defamation Law*, 45 Harv. C.R.-C.L. L. Rev. 261 (2010).

For example, each year, congregations in The Church of Jesus Christ of Latter-day Saints in the southeastern United States hold a "Day of Service." The church's regional public affairs council coordinates the events and the social media efforts, including a Facebook page and tweets.[76] While no one profits from the charitable events and all participants are volunteers, the church will not post a photograph online without a publicity release.[77] Lacking such permission, even non-profit organizations that use someone else's "name, likeness or other personal attributes without permission for an exploitative purpose" may be guilty of "misappropriation."[78]

Another situation might be that in which a company's human resources department uses social media to connect with its employees. One worker unexpectedly takes extended leave, and several other employees ask questions about her absence. Through its social media tools, the company then notifies all employees that the absent worker has cancer and is not expected to return to the office. The company may have just unlawfully invaded the absent worker's privacy by revealing her private information—that is, "information about someone's personal life that has not previously been revealed to the public, that is not of legitimate public concern, and the publication of which would be offensive to a reasonable person"—without her permission.[79] The information was true, and the company was motivated by legitimate internal concerns rather than making money, but that may not protect the disclosure.

The cyber-territory in between truth and falsehood—namely opinions and advocacy—can prove especially challenging for clients, attorneys and the courts. In 2006, a Florida jury awarded an $11 million-plus verdict against a woman who criticized a referral organization for parents with international disputes. The defendant asked the organization for help removing her children from a boarding school in Costa Rica, where her ex-husband had sent them.[80] Apparently dissatisfied with the results, she posted comments on a website calling the head of the organization a "crook" and a "con artist" who committed "fraud."[81] The Florida Appellate Court later upheld the verdict.[82]

---

[76] E-mail from Karla Brandau, regional public affairs director, to local public affairs councils, *Final Stages of Media Blitz for the Day of Service* (Apr. 11, 2010, 3:24 PM) (on file with author).

[77] E-mail from Forrest Anderson, web page coordinator, to the local publicity coordinators, *Area Page Introduction Test and Photographs* (Mar. 7, 2010, 6:52 PM) (on file with author).

[78] Ardia, *supra* note 67.

[79] *Id*. Private information includes "writing about a person's medical condition, sexual activities or financial troubles." *Id*.

[80] *See* Laura Parker, *Jury Awards $11.3M Over Defamatory Internet Post*, USA Today, Oct. 10, 2006, *available at* http://www.usatoday.com/news/nation/2006-10-10-internet-defamation-case_x.htm (reporting the results of *Scheff v. Bock*, an unpublished case).

[81] Ardia, *supra* note 67.

[82] Bock v. Scheff, 991 So.2d 1043, (Fla. App. 4th Dist. 2008).

A few years later and a few states farther north, a disgruntled former student of a summer study-abroad program aired his complaints on a website called "ripoffreport.com." Among other things, he labeled company managers as "incompetent" and described the program as "a 100% bait and switch scam" and "all a joke."[83] The trial judge dismissed all the company's tort claims against the *pro se* defendant, finding the social media comments to be protected consumer opinions:

> [S]tatements that merely express opinion are not actionable as defamation, no matter how offensive, vituperative or unreasonable they may be. . . . Moreover, in the context of statements pertaining to issues of consumer advocacy, courts have been loath to stifle someone's criticism of goods or services. . . . The courts have recognized that personal opinion about goods and services are a matter of legitimate public concern and protected speech.[84]

In another unhappy consumer case, a blogger downloaded photographs of an insurance company's executives from the company's web site. He then morphed these photos into "Wanted" posters and posted them on his blog. The insurance company sued for copyright infringement.[85] The court ruled for the defendant, finding that the "fair use" doctrine protected the defendant. The court held that the use was "transformative" and provided a vehicle for the consumer to publicize his complaints, dismissing the insurance company's claim that it would be more difficult to use the photos in the future. True copyright infringement, according to the court, entirely negates the owner's commercial ability to use and profit from the material, while any "biting criticism" or "parody" would only suppress demand.[86]

VI. NAVIGATING THROUGH CYBERSPACE

Having helped the client understand some of the legal realities of social media communication, attorneys can then provide the client with some helpful rules for using those tools effectively.

A. Rule one: Guide the client to make an informed decision about using social media

This obligation calls on the attorney to act as counselor, rather than advocate, trusted to give more than just legal advice:[87] Guide the client to make an informed

---

[83] Intellect Art Multimedia v. Milewski, 2009 WL 2915273 (N.Y.Sup. Sept 11, 2009)

[84] *Id*. at *4 (internal citations omitted).

[85] Sedgwick Claims Management Services v. Delsman, 2009 WL 2157573 (N. D. Cal. July 17, 2009)

[86] *Id*. at *6-7 (quoting Fisher v. Dees, 794 F.2d 432).

[87] *See* Model Rules of Prof'l Conduct R. 2.1 (2012) ("In representing a client, a lawyer shall exercise independent professional judgment and render candid advice. In rendering advice, a lawyer may refer not only to law but to other considerations such as moral, economic, social and political factors, that may be relevant to the client's situation.")

decision about whether the risks of social media are worth the benefits. At the risk of sounding like someone's mother, just because everyone else is doing something does not make it right for an individual client.

> [I]n the race to start leveraging these new tools, policy makers may be skipping right over important questions about what exactly they expect these new technologies to do for them and their agencies. It's critically important to ask these questions because the hurried and/or ill-conceived implementation of these new tech tools can generate as many or more problems than they solve.
>
> The unambiguous message suggested almost daily in coverage about the growing number of state and federal agencies using social networking doodads of one kind or another is this: Senior-level policy makers better get on board or risk getting left behind. Some social networking tools may indeed provide valuable capabilities that help organizations do all sorts of things better. On the other hand, used incorrectly they squander limited time and resources on unproductive, techno-enabled bureaucratic overhead.[88]

Social network tools have aptly been described as double-edged swords.[89] While some law enforcement agencies have used Twitter and Facebook to their advantage to "alert the public, seek information about crimes, and gather evidence about the backgrounds of criminal suspects,"[90] others have wrestled with challenging situations thrown their way by social media. For example, a California police department "went to great lengths to conceal a wounded officer's identity and location," only to have a retired officer (almost certainly with good intentions) disclose the information on Facebook.[91] The New Mexico police officer in the beginning illustrations admitted his comments were a lapse in judgment but only after a local television station found his Facebook page following his involvement in an on-duty fatality.[92] Other officers have seen their careless social media postings used against them as evidence in criminal trials.[93]

---

[88] Colonel Peter Marksteiner, *Does Twitter Match the Mission?*, INFO. WK., Jun. 29, 2009, http://www.informationweek.com/news/government/enterprise-architecture/showArticle.jhtml?articleID=218101782.

[89] *See* Mike Chalmers, *Deployed: Facebook Puts Family In Your Face*, MONTGOMERY ADVERTISER, Nov. 27, 2011, at 4A (reporting that the DoD is conducting a three-year study to see if the enhanced connections that families can maintain during deployments by using social media can distract members from the mission and "expose fractures in their personal relationships").

[90] Goode, *supra* note 1.

[91] *Id*.

[92] *Id*.

[93] *Id*.

U.S. Government executive-branch agencies have an additional factor to consider—the statutory restriction on using appropriated funds for publicity and propaganda[94] or "grassroots lobbying" to try to influence Congress through agency customers.[95] If an agency decides to take out a full-page newspaper advertisement, it is relatively simple for agency lawyers to review the advertisement in advance and for Congress to determine after publication whether the ad is appropriate. The Congressional Research Service (CRS), however, points to a number of characteristics that complicate attempts to policing Government social media.

First, the relative ease of social media "makes it easier for agencies to produce more public communications. . . . More communications may provide for more opportunities for an agency to transgress (inadvertently or otherwise)" the law.[96] Additionally, because social media communications often include real-time back-and-forth conversations, agency employees may make virtual off-the-cuff remarks that are inaccurate, improper or misleading.[97]

The second difficulty is finding the communication, especially when it happens in real-time, such as instant messaging or "Skyping," and results in only a fleeting digital record, if producing any record at all.[98] Once a communication is found, identifying the source and verifying the item's authenticity become hurdles. Not only are social media communications easy to create, they are easy to create anonymously,[99] even easier to forward (without tracking the original source) and relatively easy to hijack and manipulate. The CRS points out that while the Government has methods for authenticating electronic signatures, most federal social media items lack the same security measures, allowing the communications to be "commandeered by hackers or other malefactors and used to send out inappropriate content."[100]

---

[94] S*ee* 5 U.S.C. § 3107 (2010) (stating stated that appropriated funds "may not be used to pay for a publicity expert unless specifically appropriated for that purpose"). Additionally, for more than fifty years, annual appropriations acts have prohibited using appropriated funds "for publicity or propaganda purposes" that Congress has not explicitly authorized. Kevin R. Kosar, Cong. Res. Serv., R42406, Congressional Oversight of Agency Public Communications 4 (Mar. 4, 2012).

[95] Kosar, *supra* note 94, at 4 (referencing 18 U.S.C. § 1913 (2010)). "Grassroots lobbying" is defined as agencies urging citizens to influence Congress through "any personal service, advertisement, telegram, telephone, letter, printed or written matter" or other method. *Id*. (internal citations omitted).

[96] *Id*. at 9.

[97] *Id*.

[98] *Id*.

[99] *See id*. at 10 (noting that the social media items do not always have easily identifiable authors). "For example, government agencies' Twitter accounts seldom state which employees are authorized to send agency tweets." *Id., but see* Memorandum from the Deputy Secretary of Defense, to Secretaries of the Military Departments et al., subject: Policy for Department of Defense (DoD) Interactive Internet Activities, at 2-3 (8 Jun. 2007), *available at* http://www.defense.gov/webmasters/ (requiring all such activities to have "clear attribution" except for limited exceptions in the Global War on Terror").

[100] Kosar, *supra* note 94, at 9. In 2012, reported "Chinese spies" created a fake Facebook page for

Once the Government distributes a social media communication, the agency loses all control over its usage. One of the features of social media that makes it so attractive is the ease with which it can be "shared."[101] However, what if the agency's original communication, which is downloaded, uploaded, re-posted, liked, re-tweeted, and rebroadcast, also is inaccurate and/or illegal? The agency would probably find recalling, retracting, removing and otherwise rectifying that mistake to be nearly impossible. "Arguably, any time an agency publishes anything on the Internet, it could have the effect (intentionally or unintentionally) of encouraging citizens to contact Congress, especially if the communication 'goes viral'."[102]

Even assuming an agency could somehow ensure all social media communications were correct and permissible, the question still remains whether agency policy really should be disseminated in Twitter's 144 characters or in a YouTube video. As one Government Twitter user said, "Simplistic statements don't advance us."[103] Thus, the lawyer must help any client considering the use of social media to consider not only the desired results but the unintended consequences.

B. Rule two: Read the fine print and know the terms of service

If the client decides to press forward with social media, thoroughly research the service provider. Always read the fine print and become very familiar with the social media provider's terms of service. Know how the provider stores the communications and for how long. Understand the provider's policy for turning over information to law enforcement or in litigation and what the client's rights and abilities are to object or to retrieve the information itself. At a minimum, look into the following: [104]

Admiral James Stavridis, commander, Supreme Headquarters Allied Powers Europe, and sent "friend requests" to senior British officers, several of which were accepted. Rebecca Evans & Ian Drury, *Britain in Security Alert After Facebook Spies Create False Profile for Top NATO Chief to Steal Personal Data From His High-Ranking Friends*, MailOnline, Mar. 12, 2012, http://www.dailymail.co.uk/news/article-2113402/Facebook-spies-create-false-profile-Nato-chief-steal-personal-data.html.

[101] Kosar, *supra* note 94, at 10 (discussing the ease with which social media may be rebroadcast).

[102] *Id*. at 10.

[103] Inges Mergel, *Working the Network: A Manager's Guide for Using Twitter in Government*, at 14 (IBM Center for The (sic) Business of Government Using Technology Series, 2012), *available at* http://www.businessofgovernment.org/report/working-network-manager%E2%80%99s-guide-using-twitter-government, (quoting an employee of the Environmental Protection Agency); *see also* Kosar, *supra* note 94, at 9 (reporting that a former Department of Transportation chief information officer stated that "any material a federal employee publishes online can be taken as establishing or implying the establishment of a formal policy") (internal citations omitted).

[104] *A Practical Guide to Social Media for Corporate Counsel*, LexisNexis, Nov. 18, 2009, at Slide 28 [hereinafter *Social Media*], *available at* http://community.martindale.com/cfs-filesystemfile.ashx/__key/CommunityServer.Components.PostAttachments/00.00.00.53.14/A-practical-guide-to-using-social-media-for-Lawyers-CC-FINAL-9_2D00_2_2D00_09-Update.ppt.

- How well identified is the company or entity creating the site or providing the service? How does the service provider resolve disputes?
- What is the site's privacy policy? Will it sell or rent users' contact information or subject registered users to spamming or commercial solicitation?[105]
- Does the site allow anonymous posting? How does it ensure only registered and authorized members or users participate in the site?
- What control do individual users have over their privacy settings?[106]

If a client wants to reuse published material in the client's social media communications, ensure that the client does not just rely on the specific link to the online material or what is immediately visible on a website. Often, copyright notices or other re-publication restrictions are only found in a link at the very bottom of the site's home page with the other fine print. For example, on the *New York Times* website, just reading an article provides no notice of the copyright restrictions, which are actually at the bottom of the web page under the link called "Terms of Service."[107]

For Government agencies, that also means reading the organization's social media guidelines. The DoD, for example, has a "Social Media Hub" that is "designed to help the DoD community use social media and other Internet-based Capabilities (IbC) responsibly and effectively; both in official and unofficial capacities."[108] The site includes DoD policy guidance and links to service-specific guidance, as well as general social media education and training, guides for specific media, and operational and information security guidance.[109] In 2011, *The Tongue and Quill*, the Air Force's venerable handbook on military writing, added a section on social media,[110] and the Air Force Public Affairs Agency has published a guide to using social media.[111]

---

[105] *See generally id; see also* Dina El Boghdady & Hayley Tsukayama, *Facebook Tracking Prompts Call for FTC Probe*," Wash. Post, Sept. 29, 2011 (recounting lawmakers' concerns over revelations that Facebook was tracking its users' online activities even after they logged out), http://www.washingtonpost.com/business/economy/facebook-tracking-prompts-calls-for-ftc-investigation/2011/09/29/gIQAVdsP8K_story.html.

[106] *See Social Media, supra* note 104.

[107] *See* N.Y. Times, http://www.nytimes.com (last visited Feb. 7, 2013); *Terms of Service, supra* note 70.

[108] *DoD Social Media Hub*, U.S. Dep't of Def., http://www.defense.gov/socialmedia/ (last visited Feb. 8, 2013).

[109] *Id*.

[110] Memorandum from Air Force Chief Information Officer to various recipients, subject: Air Force Guidance Memorandum to AFH 33-337, *The Tongue and Quill*, 1 August 2004 (9 Nov. 2011) (on file with author). A similar memo re-issued the change in November 2012 as an interim measure until the entire handbook is revised. Memorandum from Air Force Chief Information Officer to various recipients, subject: Air Force Guidance Memorandum to AFH 33-337, *The Tongue and Quill*, 1 August 2004 (8 Nov. 2012), http://www.e-publishing.af.mil/. *The Tongue and Quill* itself is also available at this website, under "Most Viewed."

[111] *Navigating the Social Network : The Air Force Guide to Effective Social Media Use*, U.S. Air

C. Rule three: Do not delete!

How is the client going to preserve the social media records? "Astonishingly, while social media is a form of electronically stored information to which all the rules of discovery apply, very few companies collect and retain social media data created by employees on behalf of the brand."[112] Federal agencies are not much better.[113] Most organizations do have existing record-keeping plans or programs, however, and most public agencies, whether local, state or federal, have some statutory requirement to preserve their records.[114] Thus, the most logical and practical method of storing social media records is often to adapt the general framework of the client's existing information management policies.[115] For U.S. Government agencies, a good starting point is the National Archives and Records Administration (NARA), which has guidance both on managing records on the web in general and specifically on social-media platforms.[116]

Recognize, however, that "managing and preserving electronic records in general is a complex undertaking."[117] Cost goes hand-in-hand with complexity, and electronic storage is almost always more expensive than storing boxes of paper. Hard-copy records and the basic methods for storing them do not change—at worst, the client may have to move the boxes to a new warehouse. The same does not hold true for electronic storage, where technological limitations or modifications may make previously stored data inaccessible and newly stored data problematic in court.[118] Faced with such a dilemma, the Department of Justice and the Drug Enforcement Agency (DEA) recently dropped their prosecution of Florida doctor

---

Force Pub. Aff. Agency, March 2012, *available at* http://www.af.mil/shared/media/document/AFD-120327-048.pdf.

[112] Kubicki, *supra* note 34.

[113] Kosar, *supra* note 94, at 9 (asserting that Government organizations historically have not made electronic record storage a "high priority").

[114] For example, the Freedom of Information Act, 5 U.S.C. § 552 (2010), requires federal government agencies to make available information on how the agencies operate, make decisions, procedural and substantive rules and other areas that make government operations more transparent to the public. In 1996, Public Law No. 104-231, or the "Electronic Freedom of Information Act" expanded FOIA coverage to electronic records. 5 U.S.C. § 552 (2010).

[115] Kubicki, *supra* note 34.

[116] Nat'l Archives & Rec. Admin., *NARA Guidance on Managing Web Records*, Jan. 2005, http://www.archives.gov/records-mgmt/policy/managing-web-records-index.html; NARA Bulletin 2011-02, to Heads of Federal Agencies, subject: Guidance on Managing Records in Web 2.0/Social Medial Platforms, Oct. 20, 2010, http://www.archives.gov/records-mgmt/bulletins/2011/2011-02.html.

[117] Kosar, *supra* note 94, at 9.

[118] *See* John Patzakis, *Overcoming Potential Legal Challenges to the Authentication of Social Media Evidence*, Apr. 2, 2013, at 1, *available at* http://articles.forensicfocus.com/2012/04/02/overcoming-potential-legal-challenges-to-the-authentication-of-social-media-evidence/ (warning that the available digital forensic tools are not able to "collect social media in a scalable manner while supporting litigation requirements such as the capture and preservation of all key metadata . . . and chain of custody").

who allegedly committed $6.5 million in Medicaid fraud.[119] Their reason: the two terabytes of evidence in the case, which ate up five percent of the DEA's storage capacity, was too expensive for the Government to maintain. [120] The DEA could have upgraded its storage, but doing so might have jeopardized the legal integrity of the electronically stored evidence.[121]

D. Rule four: Protect your good name

Clients must also understand how to protect their company identity or brand. Facebook allows links to an organizational Facebook page, but what if a dispute arises between two users over the rights to use very similar names?[122] Also, since late 2011, companies have been able to register domain names with a .xxx ending (rather than other domains such as .com, .net, and .org.).[123] While aimed at the adult entertainment industry, these domain names pose the risk that "brands may be compromised in a way that not only is potentially harmful to business, but also may be very embarrassing."[124] Disney, for example, very zealously guards its domain and brand name—online users who type in "magickingdom.com" are automatically redirected to the Disney World site. A Google search for "magic kingdom" returns page after page of nothing but Disney-related links.[125] One can imagine both the adult-entertainment value of "MagicKingdom.XXX" and the resulting legal barrage from Disney should the trademark's image be sullied. Unlike many organizations, however, Disney has the wherewithal to engage in costly and time-consuming litigation to fight infringement.[126]

For clients with fewer resources, the best course is to monitor both the domain name and what is being said about the organization. A "domain watching service" is much like a credit-monitoring program, reporting anything that could be adverse online material.[127] For clients who prefer the do-it-yourself method, a monitoring method could be as simple as "Google Alerts," which provide email

---

[119] Ryan J. Foley, *Fugitive Skates on Charges for Bulk of Evidence*, Az. Rep., Aug. 19, 2012, at A15.

[120] *Id.* "Two terabytes is enough to store the text of 2 million novels, or roughly 625 copies of 'War and Peace'." *Id*.

[121] *Id.*

[122] *See Social Media, supra* note 104, at Slide 35 (noting that an "open question remains regarding how Facebook will resolve disputes").

[123] Jennifer L. Elgin, *Protect Your Brand in "Triple X" Domain by October 28*, Wiley Rein Newsl: Gov't Cont. Update, Sept. 26, 2011, http://www.wileyrein.com/publications.cfm?sp=articles&id=7492.

[124] *Id*.

[125] Google search conducted Feb. 8, 2013 (results on file with author).

[126] *See* Elgin, *supra* note 123 (suggesting that infringement lawsuits are one of the more expensive methods to protect domain names).

[127] *See id*. (comparing a domain watching service to an "insurance policy "to discover potentially damaging internet uses").

updates of the relevant Google results, based on the user's chosen query or topic, source of publication, delivery method, and frequency of results. [128]

E. Rule five: Assess the client's ability to engage customers

Social media is not a "click-and-forget" effort. Any organization seeking to engage customers or clients through social media should first take stock of its ability to monitor the social media interaction and, when necessary, respond to questions and concerns.[129] Both the time demand and figuring out methods of appropriate interaction can be challenging.[130] For example, in its first week of operation, "We the People," an online site for citizens to petition the Obama administration, found itself overwhelmed by petitioners. Initially, online petitions had to gather at least 5,000 signatures within thirty days to merit an official White House response—a threshold reached by at least thirty petitions within the first seven days.[131] In October 2011, the White House raised the requirement to 25,000 signatures, then to 100,000 in January 2013[132].

As a general rule, an organization should only seek comments through social media outlets if it has first determined that it has the capacity to respond. "It's usually not good to ask for input if you're not able to respond to it effectively. Otherwise, you're just alienating those who have expressed their opinions."[133] If a Government organization is not actively monitoring a social media site, then the organization should post a blanket statement to that effect, similar to the disclaimer contained in automatically generated e-mails.[134] Such a practice can go a long way toward setting realistic customer expectations which, in turn, can reduce the number of customer complaints posted on the Internet for the world to see.

These guidelines are all relatively common-sense and practical to implement. Determining the organization's social media policies dealing with employee use can be far more challenging.

---

[128] Google, *Google Alerts*, http://www.google.com/alerts?hl=en (last visited Feb. 8, 3013).

[129] See Joseph Marks, Think Before You Tweet (May 14, 2012), http://www.nextgov.com/mobile/2012/05/think-you-tweet/55728/.

[130] *See* Mergel, s*upra* note 103, at 14 (noting that "many public managers struggle with effective use" of social media).

[131] Joseph Marks, *White House Grapples With a Flood of Online Petitions*, NextGov.com (Oct. 4, 2011), http://www.nextgov.com/technology-news/2011/10/white-house-grapples-with-a-flood-of-online-petitions/49885/.

[132] Joseph Marks, W*hite House Raises We the People Response Threshold to 100,000 Signatures*, NextGov.com (Jan. 16, 2013), http://www.nextgov.com/emerging-tech/2013/01/white-house-raises-we-people-response-threshold-100000-signatures/60700/.

[133] Marks, *supra* note 131 (quoting Randy Paynter, founder of an online petition site).

[134] Marks, *supra* note 3.

F. Rule six: Establish a defensible social media use policy for the organization

As one commentator notes, the tension comes in striking "the right balance between participating in social media and self-preservation. . . . [C]ompanies that enact broad bans on social media miss an opportunity to allow their employees to engage with public or their peers positively. On the other side of the spectrum, free access often creates huge liability traps."[135] Organizations have a legitimate interest in ensuring that social media communications do not harm their organization's interests in a way that would prevent them from carrying out their mission—whether that mission is to make money or to serve the public.

Once again, some aspects of a policy seem relatively straightforward, for example, employees should not reveal confidential or proprietary information outside the organization. And once more, helping organizations and their members understand the distinction between their intentions and the actual results is crucial. Turning back to the federal worker discussed at the beginning of this article, she clearly did not intend to reveal confidential attorney-client information; rather, she was seeking advice from her peers in what she perceived to be a low-threat environment. However, in doing so, she risked waiving the attorney-client privilege. After thirty-seven posts discussing the federal worker's question and advice given by the agency lawyer, a self-identified government attorney wrote:

> I have some concerns about the sharing of specific, detailed advice given to an agency customer by the agency counsel . . . [W]hen it is shared in a public forum such as this, that attorney-client privilege is breached and the advice is no longer privileged and confidential and could be disclosed in a forum such as a bid protest . . . . Don't think unsuccessful offerors don't scour the Internet for comments such as these. I know they do.[136]

The forum moderator agreed and revised the post, reminding participants that posts are to be couched in hypothetical terms.[137]

Other employee-related policies can be far more challenging to develop. In a 2011 report, NLRB said such policies "have presented emerging issues concerning the protected and/or concerted nature of employees' Facebook and Twitter postings . . . and the lawfulness of employers' social media policies and rules."[138] Much

---

[135] Kubicki, *supra* note 34.

[136] Wifcon Forum, *supra* note 2.

[137] *Id*.

[138] NLRB 2011, *supra* note 45, at 2. Everyone involved in developing social media policy should read the report and the two that followed it in 2013. Nat'l Lab. Rel. Board, *Report of the Acting General Counsel Concerning Social Media Cases*, Jan. 24, 2012 [hereinafter NLRB Jan. 2012], available at http://www.nlrb.gov/news/acting-general-counsel-issues-second-social-media-report; Nat'l Lab. Rel. Board, *Report of the Acting General Counsel Concerning Social Media Cases*,

of the controversy springs from Section 7 of the National Labor Relations Act,[139] which protects an employee's right "to form, join or assist labor organizations . . . and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection."[140] Employers are not supposed to "interfere with, restrain, or coerce" employees who exercise their Section 7 rights.[141]

In the first NLRB case cited in the OGC's 2011 report, an employee of a nonprofit social services agency had a conflict with the agency's advocate for domestic violence victims, and so another coworker suggested she schedule a meeting with the employer's executive director. To prepare for the meeting, the employee posted comments about her problems with the advocate on her Facebook page and asked her other coworkers for input.[142] Four coworkers responded, peppering some of their comments with swearing and sarcasm.[143] The advocate also responded and complained to the executive director that the comments were "cyber-bullying" and harassment. The agency discharged the employee who made the initial post and the other four coworkers (but not the advocate) who responded.[144] The NLRB ruled that the terminations were unlawful, holding that the

> Facebook discussion here was a textbook example of concerted activity, even though it transpired on a social network platform. The discussion was initiated by the one coworker in an appeal to her coworkers for assistance. Through Facebook, she surveyed her coworkers on the issue of job performance to prepare for an anticipated meeting with the Executive Director, planned at the suggestion of another employee. The resulting conversation among coworkers about job performance and staffing level issues was therefore concerted activity.[145]

The NLRB reached similar conclusions in other cases in which workers criticized their employers on Facebook, as long as the comments grew out of "concerted activity," *not* "individual gripes."

Contrast these cases with others where the NLRB determines an employee was acting on his own and not in furtherance of concerted activity with his coworkers.

May 30, 2012 [hereinafter NLRB May 2012], *available at* http://www.nlrb.gov/news/acting-general-counsel-releases-report-employer-social-media-policies.

[139] 29 U.S.C. §§ 151-169 (2010).

[140] *Id*. at § 157.

[141] *Id*. § 158(a).

[142] NLRB 2011, *supra* note 45, at 3. The NLRB report does not identify the cases, employers or employees.

[143] *Id*. at 4.

[144] *Id.* at 3.

[145] *Id*. at 4.

In one such case, an employee posted comments on Facebook criticizing the new assistant manager at the store where he worked, complaining about being the new manager's "tyranny" and about being "chewed out" and describing the manager using a Spanish obscenity.[146] The NLRB concluded that the posting was not a concerted activity because the employee did not try to initiate group action among his co-workers, nor did the posting grow out of any such group activity.[147]

In a scenario with a slightly different twist, the NLRB upheld the firing of an employer who posted messages on her U.S. senator's Facebook "wall."[148] In that case, the employee worked for a company that provided fire protection and medical transport response services. After her senator announced on Facebook that four fire departments in his state had received federal grants, the employee complained on the senator's Facebook wall about her company's low wages and equipment deficiencies and described an incident where an untrained crew responded to an emergency call. The company terminated her for "publicly posting disparaging remarks about the Employer and confidential information about its response to a service call."[149] The NLRB found that the employee did not engage in protected concerted activity—that is, she made no attempt to get other employees involved nor did she try to take workplace complaints to management. She also admitted that she did not expect the senator to correct the situation. Instead, "she was merely trying to make a public official aware of the condition of emergency medical services in her state."[150]

So what is an employer to do? One expert offered this bottom line: "[T]hink twice before reprimanding, disciplining or terminating an employee because his or her tweet hurt your feelings."[151] Additionally, organizations should not try to control employees' association with other workers or broadly limit what employees may discuss. The NLRB struck down as ambiguous and overly broad a policy that warned employees to "[t]hink carefully about 'friending' co-workers . . . on external social media sites" because "what you say in your personal social media channels could become a concern in the workplace."[152] Similarly, the NLRB overturned a policy

---

[146] *Id.* at 17-18.

[147] *Id*.

[148] *Id.* at 15.

[149] *Id.* at 16.

[150] *Id*. The case here involved a private employer, with no allegations of fraud. In other circumstances, communications with members of Congress may enjoy more protections. *See, e.g.,* 10 U.S.C. § 1034 (2010), which prohibits any person from restricting a servicemember's communication with Congress, "Unless the communication is unlawful or violates a regulate necessary to the security of the United States;" Thomas M. Devine, *The Whistleblower Protection Act of 1989: Foundation for the Modern Law of Employment Dissent, 51* Admin. L. Rev. 531 (1999) (examining the evolution of protections available to those who report wrongdoing or fraud in government).

[151] Brian Hall, *An Appeal for Cooler Heads on NLRB's Social Media Policy Enforcement*, Emp. L. Rep., Apr. 25, 2011, http://www.employerlawreport.com/2011/04/articles/workforce-strategies/an-appeal-for-cooler-heads-on-nlrbs-social-media-policy-enforcement/#axzz1ZMqtAnN5.

[152] NLRB May 2012, *supra* note 138, at 8.

that prohibited employees from commenting on any legal matters or discussing any controversial topics online.[153] The NLRB did, however, uphold in its entirety a policy that contained many of the same principles as unlawful policies, primarily because it provided specific examples. The board said:

> [R]ules that are ambiguous as to their application as to Section 7 activity and that contain no limiting language or context to clarify that the rules do not restrict Section 7 rights are unlawful. In contract, rules that clarify and restrict their scope by including examples of clearly illegal or unprotected conduct, such that they could not reasonably be constructed to cover protected activity, are not unlawful.[154]

Thus, the key for organizational policies is to, first, make clear that the organization is not attempting to stifle protected Section 7 discussions on terms and conditions of employment. An organization must be able to articulate the purpose and rationale for any policy and then demonstrate how each facet of the policy contributes to achieving the desired goals.[155] For example, the NLRB struck down an employer's social media policy that banned workers from using the company's name, address or other information in their personal social media use. In that particular case, "The Employer offered no explanation as to why employees could not identify the Employer on their personal profiles, but even assuming that it had a legitimate interest in preventing disclosure of certain protected company information to outside parties, the ban was not narrowly drawn to address those concerns."[156] Ultimately, the policy failed because it harmed the employees' Section 7 rights.[157]

Secondly, be specific—do not just talk in broad generalities that urge employees to be nice. The NLRB pointed out that in certain contexts, an employer's rule to "Be Respectful" would be unlawful. However, the rule becomes proper when accompanied by examples of prohibited conduct, such as "offensive posts meant to intentionally harm someone's reputation" or posts that could contribute to a hostile work environment.[158] These NLRB decisions mean that the attorney's job in many

---

[153] *Id.* at 10.

[154] *Id*. at 20.

[155] Some companies in specialized fields with statutory or regulatory restrictions on information release may be able to justify a stricter policy—for example, the securities industry. "Information that could affect a public company's stock price, or is otherwise important to investors, should not be discussed through social media unless it has previously been announced in a filing with the Securities and Exchange Commission." Andrew M. Nick, *The Use of Social Media in Corporate Communications*, Sept. 2011, http://www.fredlaw.com/articles/corporate/corp_1109_amn.html.

[156] NLRB 2011, *supra* note 45, at 21.

[157] *Id*.

[158] NLRB May 2012, *supra* note 138, at 20.

cases may be to help the client reach that level of specificity, by understanding what it is that the client really wants to prohibit and how to describe it.

For Federal Government organizations, the political arena is another area that employers and employees must both understand—and the rules apply to both what individual workers do online and what the organization itself may do with social media. Since 1939, The Hatch Act[159] has limited the permissible extent of political activities for civilian employees. Generally, the rules apply to the use of official authority and on-duty activity, and generally, they are relatively straightforward, such as those prohibiting most federal employees from distributing campaign materials in the Government workplace or soliciting a Government contractor to support a certain political candidate.[160] However, when it comes to off-duty social media use, the rules become less clear. For example, the rules "prohibit federal employees from using their official titles while engaging in 'political activity'."[161] Does that rule, therefore, bar a U.S. Government civilian worker from creating a personal Facebook page, identifying himself as a federal employee by his official title, and also specifying his political views? According to the U.S. Office of Special Counsel (OSC), the organization tasked with enforcing the Hatch Act, [162] it does not.[163] The OSC does not consider "the inclusion of a federal employee's official title or position on [his] social media profile, without more, to be an improper use of his official authority to bolster the statement he posts."[164]

Other permitted activities include off-duty partisan political advocacy on social media, as long as that activity does not ask for contributions or target subordinates; liking the Facebook page of a partisan political candidate; and even allowing someone to post comments on the employee's social media that the employee himself could not make.[165] Contrast this rule with the case against Stein, the former Marine discussed earlier.[166]

Stein's Armed Forces Tea Party site at one point included a post that labeled the president as "Jackass number one." Stein denied posting the comment but admitted that he let it remain. Did he have an affirmative responsibility to police his site under DoDD 1344.10 or any other provision of military law? In other

---

[159] 5 U.S.C. §§ 7321–7326 (2010).

[160] *Less Restricted Employees—Political Restrictions and Prohibited Activities*, U.S. Off. of Special Couns.; http://www.osc.gov/haFederalLessRestrisctionandActivities.htm (last visited Feb. 11, 2013).

[161] *Id*.

[162] *OSC's Role (Hatch Act)*, U.S. Off. of Special Couns., http://www.osc.gov/haFederalOSCrole.htm (last visited Feb. 11, 2013).

[163] *Frequently Asked Questions Regarding Social Media and the Hatch Act*, U.S. Off. of Special Couns., Apr. 4, 2012, at 1, *available at* http://www.dod.mil/dodgc/defense_ethics/resource_library/guidance.htm.

[164] *Id*. at 2.

[165] *See id.* at 3-4 (describing the limits of permissible political activity for individual employees).

[166] S*ee supra* notes 17-23 and accompanying text.

words, can a military member face disciplinary action not for his own conduct but for failing to adequately monitor others using a medium he provides?

While Stein's supporters characterized the situation as a constitutional issue, the question of whether DoDD 1344.10 actually applies to online political speech received little attention except from his defense lawyers, who said, "There is no basis in this case. Sgt Stein has broken no law."[167] They argued that the DoD policy not only improperly infringed on Stein's freedom of expression in his private capacity, it also was vague and misunderstood even by senior officials.[168] They have a point.

DoDD 1344.10 itself never uses the word "online" or mentions computers or the Internet, except for one sentence stating that electronic copies of the publication are available on the web.[169] Given that, does a Facebook post fall within the prohibition against publishing partisan political material? Is engaging in an online forum legally the same as participating in radio or television programs or other group discussions? Does it make a difference that the radio or television programs are meant to be broadcast, while Stein intended his discussion to be a "private Internet chat" that just "happened to go public and go viral"?[170] The directive would have permitted Stein to put a political bumper stick on his car, which he certainly would have driven in public, quite possibly in uniform.[171] He could have written a letter to the editor expressing his views and identifying himself as an active-duty servicemember, as long as he clearly stated that the views expressed were his and his alone.[172] According to the directive, he could have attended a partisan political rally in his personal capacity and out-of-uniform.[173] Substantively, how does that differ from Stein's private (but seen by others) Facebook chats or website posts, assuming he followed the same restrictions? Admittedly, his comments were not respectful, but "contemptuous speech" toward the President by enlisted members is not a crime.[174]

Within weeks of Stein's discharge, the DoD Public Affairs (PA) office published guidance for political campaigns and elections that includes a section covering "online/social media" that applies to active-duty servicemembers.[175] Under

---

[167] Julie Watson, *Board Seeks Marine's Dismissal Over "Contemptuous" Anti-Obama Facebook Comments*, Christian Sci. Monitor (Apr. 6, 2012), http://www.csmonitor.com/USA/Latest-News-Wires/2012/0406/Board-seeks-Marine-s-dismissal-over-contemptuous-anti-Obama-Facebook-comments (quoting Marine Captain James Baehr, Stein's military defense attorney).

[168] *Id.*

[169] DoDD 1344.10, *supra* note 19, para. 6.

[170] Rooney, *supra* note 17.

[171] DoDD 1344.10, *supra* note 19, para. 4.1.1.8.

[172] *Id*. at para. 4.1.1.6.

[173] *Id*. at para. 4.1.1.9.

[174] The criminal proscription against "contemptuous speech" about the President only applies to commissioned officers and not to enlisted members such as Stein. UCMJ, art. 88 (2010).

[175] Memorandum from the Office of the Assistant Secretary of Defense for Public Affairs , subject:

the guidance, an active-duty service member "may generally express his or her own personal views on public issues or political candidates via social media platforms" (similar to writing a letter to the editor of a newspaper), as long as the writer includes the caveat that "the views expressed are those of the individual only," not the DoD.[176] Servicemembers may "like" a partisan political candidate's Facebook page or "follow" a partisan political Twitter account, they may *not* suggest that others "like," "friend," or "follow" any political group or candidate.[177] The PA guidance then goes onto say that troops "may not post or make direct links to a political party, partisan political candidate, campaign, group, or cause because such activity is the equivalent of distributing literature on behalf of those entities or individuals," which DoDD 1344.10 prohibits.[178] Further, active-duty servicemembers "may not post or comment on the Facebook pages or 'tweet' at the Twitter accounts of a political party, or partisan political candidate, campaign, group, or cause, as such activity would be engaging in partisan political activity through a medium sponsored or controlled by said entities."[179]

The guidance, however, does not provide any support for the conclusion that certain online activities equate to "distributing literature." How does posting an online link to a political party differ so much from a bumper sticker encouraging others to vote in line with a party's views? As its basis for the prohibition against posting on partisan Facebook pages or suggesting that others follow a political candidate, the PA guidance directs readers to see DoDD 1344.10 "for further clarification."[180] However, that search for clarification seems destined to end in failure because the DoD directive does not address online activities in any form. The reality, it seems, is that these social media guidelines are the interpretation of DoDD 1344.10 from a public-affairs perspective, rather than legally binding and potentially punitive rules.[181]

This is not to say that the Marines were wrong to discharge Stein, or that the DoD Public Affairs guidance is incorrect. It does, however, point out the need for attorneys to be involved in many areas that are not traditionally their bailiwick. Additionally, lawyers should not only assist clients in crafting the policy but should continue with education, implementation and enforcement. No matter how finely

---

2012 DoD Public Affairs Guidance for Political Campaigns and Elections, para. 9.4.1 (May 2, 2012) [hereinafter DoD Public Affairs Guidance], available at http://www.dod.mil/dodgc/defense_ethics/resource_library/guidance.htm.

[176] *Id.* at para. 9.4.2.

[177] *Id.* at para. 9.4.3.

[178] *Id.*

[179] *Id.*

[180] *Id.*

[181] Contrast the Hatch Act guidance discussed earlier, which came directly from the legal office charged with enforcing the act and thus does carry some legal weight. *See supra* notes 160-165 and accompanying text. The Public Affairs guidance provides no indication of any legal coordination or imprimatur.

tuned a social media policy may be, it serves no purpose if employees have received no training and do not comprehend it. Both employer and employee must have clear expectations and a good understanding of what the policy is intended to do and how it will be enforced.

VII. CONCLUSION

As actor John Wayne once said, "Life is tough, but it's tougher when you're stupid."[182] Because life and the law involve people, people will continue to use social media to say and do stupid things. Early involvement and solid guidance from attorneys can help ensure that the stupidity does not make life quite so tough for organizational clients.

[182] John Wayne, BRAINYQUOTE.COM, http://www.brainyquote.com/quotes/quotes/j/johnwayne109679.html (last visited Feb. 6, 2013).

THE BIG PAYBACK: HOW CORRUPTION TAINTS OFFSET AGREEMENTS IN INTERNATIONAL DEFENSE TRADE

Lieutenant Colonel Ryan J. Lambrecht[*]

[*] Lt Col Lambrecht serves in the U.S. Air Force Judge Advocate General's Corps, where he currently works as Chief of the Source Selection and Acquisitions Branch, Contract Law Field Support Center. He wishes to thank his wife, Nozomi, for her limitless understanding and support, and Dean Jessica Tillipman and Professor Susan Ringler for their insight and guidance. The views expressed in this paper are solely those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense or U.S. Government.

I. INTRODUCTION

When Parliament passed the U.K. Bribery Act 2010, the Act was prompted in no small part by defense industry corruption.[1] A Serious Fraud Office (SFO) investigation of BAE Systems (a major British aerospace firm) which discovered that for over twenty years, BAE paid £6 billion ($9.7 billion) in bribes to members of the Saudi royal family in exchange for defense contracts totaling £43 billion ($69.4 billion).[2] BAE paid for its bribes, in part, by submitting fraudulently inflated bills to the Saudi government. In one contract, BAE inflated a contract by thirty-two percent to pay for £600 million ($970 million) in bribes.[3] In short, BAE bribed the Saudi royal family by stealing from the Saudi treasury.[4] As the SFO further investigated BAE, more allegations of bribery emerged, including an allegation of 24 million Rand ($3 million) in BAE bribes to South African officials.[5] The allegation centered on an arcane practice in defense trade—the use of a reciprocal transaction, or "offset," in the satisfaction of BAE's South African contract.[6] Specifically, BAE allegedly bribed South African officials to not only receive a fighter jet procurement, but also to be released from its offset obligations.[7] As the South African government continues investigating BAE,[8] anti-corruption advocates are now asking their own questions: what are defense offsets, and how susceptible are they to corruption?

---

[1] Joint Committee on the Draft Bribery Bill, Draft Bribery Bill, 2008-9, H.L. 115-I, H.C. 430-I, at 13 (U.K.); *see* Ministry of Justice, Bribery Act 2010, 2010, Circular 2011/05, at 2 (U.K.) (passage of U.K. Bribery Act 2010).

[2] David Leigh & Rob Evans, *Secrets of Al-Yamamah*, The Guardian, http://www.guardian.co.uk/baefiles/ page/0,,2095831,00.html (last visited Aug. 7, 2012) [hereinafter Leigh & Evans, *Al-Yamamah*]; David Leigh & Rob Evans, *Nobbing the Police*, The Guardian, http://www.guardian.co.uk/baefiles/page/ 0,,2098531,00.html (last visited Aug. 7, 2012); *see* The Money Converter, http://themoneyconverter.com/gbp/usd.aspx, (last visited May 9, 2012), for conversion from U.K. pounds to U.S. dollars. The contracts in question were collectively called the "Al Yamamah" contracts, and involved the sale of fighter aircraft and jet trainers, the construction of two air bases, and the provision of a host of other equipment and services by BAE Systems for the government of Saudi Arabia. David Pallister, *The Arms Deal They Called The Dove: How Britain Grasped The Biggest Prize*, The Guardian, Dec. 14, 2006, at 9. The deal was entered into in 1988, and was eventually worth a total of £43 billion ($69.4 billion). Leigh & Evans, *Al-Yamamah*; The Money Converter.

[3] Leigh & Evans, *Al-Yamamah*, *supra* note 2; *see* The Money Converter, *supra* note 3, for conversion from U.K. pounds to U.S. dollars.

[4] Pallister, *supra* note 3, at 9.

[5] Sam Sole & Stefaans Brümmer, *BAE's 'Bribery' Channel*, Mail & Guardian (South Africa), (Jun. 24, 2011, 12:00am), http://mg.co.za/article/2011-06-24-baes-bribery-channel; Ivor Powell, '*Consultant' at Centre of Arms Bribery Scandal*, Argus Weekend (South Africa), Jun. 19, 2011, at NEWS, pg 4. *See* The Money Converter, *supra* note 3, for South African Rand/U.S. Dollar conversion.

[6] Sole & Brümmer, *supra* note 6; Stephen Martin, *Countertrade and Offsets: An Overview of the Theory and Evidence*, *in* The Economics of Offsets: Defence Procurement and Countertrade 15, 31 (1996).

[7] Sole & Brümmer, *supra* note 6.

[8] *South Africa Reopens 1999 Arms Deal Investigation*, BBC, (Sep. 15, 2011, 8:44 PM), http://www.bbc.co.uk/news/world-africa-14939077.

A defense offset is an agreement to do specific future business in a country in exchange for the award of a defense contract.[9] In a 2010 report, Transparency International (TI) concluded defense offsets are highly susceptible to corrupt activity due to their high transactional value, lack of transparency, and technical nature, and that these risk factors enable companies to bribe government officials in exchange for the creation of offset requirements, award of offset contracts, and theft of offset funds.[10] However, TI's report only scratched the surface of how corruption works in defense offsets.

To clarify how corruption taints offset transactions, this article argues that fraudulently inflated offset valuations, improper sole sourcing, and lack of transparency are the key elements that make defense offsets exploitable for corruption. To prevent and detect offset corruption, the international community and defense industry must both take action to curb abusive offset practices. Specifically, the Organization for Economic Cooperation and Development (OECD) should begin negotiations for a convention to set out basic standards for offset procurements. In addition, defense vendors should heighten their due diligence standards and increase electronic audits of offset documents.

To analyze the problem of defense offset corruption, Part II of this article first describes the corruption risks offsets create, as well as the basics of how offset transactions work. Part III summarizes offset regulations in the two largest defense markets, the United States and European Union, as well as the World Trade Organization's (WTO) offset rules. Part IV discusses criminal statutes that punish bribery and false claims in offset transactions. These statutes include the Foreign Corrupt Practices Act (FCPA), U.K. Bribery Act 2010, and False Claims Act. Part V analyzes how corrupt actors can manipulate offset transactions through valuation, competition, and transparency flaws. Finally, Part VI proposes new anti-corruption initiatives for the OECD and defense industry vendors.

II. DEFENSE OFFSETS AND THEIR CORRUPTION RISKS

Offsets are a complex and arcane aspect of defense trade. Defense offsets are compensation agreements where a defense vendor promises to do specific future business in a country in exchange for the award of a government procurement contract.[11] It is a reciprocal transaction that allows the purchasing government's economy to recoup, or "offset," some of the procured defense item's purchase

---

[9] Martin, *supra* note 7, at 31; U.S. Dep't Of Commerce, Offsets in Defense Trade: Sixteenth Study 1 (2012) [hereinafter Dep't of Commerce, Sixteenth Study]; U.S. Gen. Accounting Office, GAO/NSIAD-96-65, Military Exports: Offset Demands Continue To Grow 1 (1996) [hereinafter Gen. Accounting Office, GAO/NSIAD-96-65].

[10] Transparency Int'l, Defence Offsets: Addressing the Risks of Corruption & Raising Transparency 18, 43 (2010) [hereinafter Transparency Int'l, Defence Offsets].

[11] Martin, *supra* note 7, at 31; Dep't of Commerce, Sixteenth Study, *supra* note 10, at 1; Gen. Accounting Office, GAO/NSIAD-96-65, *supra* note 10, at 1.

price.[12] An offset agreement is made between a defense vendor and a purchasing government, but it involves the vendor placing work with a company located in the purchasing country.[13] Vendors and governments agree to offsets within the broader context of negotiating the sale of a major weapon system, usually in the aerospace and communications sectors.[14] During these negotiations, vendors may offer offsets as an inducement, or purchasers may set them as a purchase condition.[15] The business occurring in an offset arrangement is dependent on the successful negotiation of the defense sale. Without the defense sale, the offset transaction either would not occur on the open market, or would occur at a much higher cost.[16] However, without the inducement of an offset arrangement, the main defense sale may also not occur for a particular vendor, due to other defense firms outbidding the losing firm with more lucrative offset deals.[17]

The use of offsets began in 1961, when the United States required West Germany to buy U.S. weapons to offset the economic impact of maintaining U.S. military forces in Germany.[18] However, by the early 1970s, Western European countries began conditioning their purchases of American goods on incentives such as job creation and technology transfer.[19] By the 1980s, offset arrangements were present internationally, and countries such as South Korea asserted high offset demands. As an example, in a heated competition between General Dynamics and McDonnell-Douglas, Korean offset demands escalated from thirty percent of the contract's value to sixty percent.[20] At the present time, offsets are an integral part of negotiations in defense trade. In an average contract, a U.S. vendor agrees to an offset worth 63.5 percent of the price of the defense sales contract.[21]

Offsets, however, are prone to corruption. An offset may be exploited for numerous illegal purposes, including bribes to generate offset requirements, bribes

---

[12] *See* Jurgen Brauer & J. Paul Dunne, *Introduction, in* Arms Trade And Economic Development 1, 3 (2004) (citing Bernard Udis & Keith E. Maskus, *Offsets as Industrial Policy: Lessons from Aerospace, in* Defence Economics, Vol. 2, No. 2, at 152 (1991) (stating that offsets allow purchasing governments to recoup, or offset, some of their investment).

[13] Brauer & Dunne, *supra* note 13, at 4.

[14] Dep't of Commerce, Sixteenth Study, *supra* note 10, at 7-8.

[15] Gen. Accounting Office, GAO/NSIAD-96-65, *supra* note 10, at 2.

[16] Lloyd J. Dumas, *Do Offsets Mitigate or Magnify the Military Burden?*, *in* Arms Trade And Economic Development 16, 22 (Jurgen Brauer & J. Paul Dunne eds., 2004).

[17] Dep't of Commerce, Sixteenth Study, *supra* note 10, at 1; *see Foreign Military Sales and Offsets: Hearing Before the H. Comm. on Energy and Commerce*, 99th Cong. 3 (1985) (statement of Frank C. Conahan, General Accounting Office) (discussing offsets as a marketing tool for foreign military sales).

[18] Bernard Udis and Keith E. Maskus, *US Offset Policy, in* The Economics of Offsets: Defence Procurement and Countertrade 357, 358 (Stephen Martin ed., 1996).

[19] *Id*. at 359; Martin, *supra* note 7, at 34.

[20] Udis & Maskus, *supra* note 19, at 363.

[21] Dep't of Commerce, Sixteenth Study, *supra* note 10, at 3.

to gain offset business, and bribes to satisfy offset obligations.[22] Additionally, offset parties may submit fraudulent invoices for sham transactions.[23] Offsets are susceptible to corruption due to four main reasons: they offer high-value inducements that are often tangential to the subject of a defense sale, they promote disparate policy goals that make them difficult to monitor, they use complex and opaque rules that frustrate transparency, and they require the use of consultants who are often closely connected to government officials.

A. Questionable Inducements in Competitive Sales

Offsets are vulnerable to corruption because they distribute large sums of money as incentives in highly competitive, negotiated government procurements. Although these procurements involve major weapons systems costing billions of dollars, much of the offset work incentivizing these sales bears no direct relation to the basic defense item.[24] This disconnect between the subject of defense procurements and the subject of defense offsets raises a suspicion that offset incentives contain improper or corrupt inducements.

Defense offsets, like defense procurements as a whole, pose an attractive target for corruption due to their large monetary values.[25] For example, U.S. companies entered into over eleven thousand offset transactions worth more than $56 billion between 1993 and 2010.[26] Additionally, offsets constitute a high percentage of the value of defense sales. For example, in February 2012, the Indian government agreed to purchase $20 billion in fighter jets from the French company Dassault, and as part of this deal, Dassault agreed to offset obligations worth half the contract's value.[27]

Another driver of offset corruption is the competitive nature of international defense sales. Purchasing governments exert considerable leverage to extract offset concessions from vendors because defense sales are rare and lucrative.[28] The life cycle of a major weapons system can run up to thirty years,[29] and the profit

---

[22] Transparency Int'l, Defence Offsets, *supra* note 11, at 18-19.

[23] *Id.*

[24] *See generally* Dep't of Commerce, Sixteenth Study, *supra* note 10, at 3-4, 7-8 (stating that defense sales and offset dollar amounts, indirect offsets accounting for 59.04 percent of U.S. offset transactions between 1993 and 2010, top four defense sectors participating in offsets).

[25] Transparency Int'l, Defence Offsets, *supra* note 11, at 4. From 1993 to 2010, the accompanying defense sales contracts numbered 763, and were worth $111 billion. *Id*. at 3.

[26] Dep't of Commerce, Sixteenth Study, *supra* note 10, at 4.

[27] James Lamont & James Boxell, *India's Choice of a New Fighter Jet Reveals Hard Truths About a Promising Market—and the Risks for Politicians and Executives of Misreading It,* Financial Times (USA ed.), Feb. 7, 2012, at 7.

[28] *See* Travis Taylor, *Using Procurement Offsets as an Economic Development Strategy, in* Arms Trade And Economic Development 30, 31 (Jurgen Brauer & J. Paul Dunne eds., 2004) (purchasing government pressure to extract offset concessions).

[29] Jeffrey P. Bialos et al., Fortresses and Icebergs: The Evolution of the Transatlantic Defense

from these systems' sales have traditionally been high.[30] Moreover, although the defense industry in the United States and European Union has undergone substantial consolidation since the 1990s, there remain enough defense firms internationally to offer fierce competition.[31] For example, the above-mentioned Indian fighter jet procurement initially involved rival offers from Boeing, Lockheed Martin, Dassault, and an EADS/BAE/Alenia Aeronautica consortium.[32] In such an environment, offerors are under considerable pressure to outbid their rivals' offset proposals.[33]

Another factor motivating offset corruption is that they have been a key deciding factor in past defense procurements. The offset laws of countries such as Poland, Hungary, Greece, and Portugal make offsets an award criterion in defense procurements.[34] These laws make offset only one of several criteria,[35] but even if offsets have relatively minor weight as a criterion, they can still be pivotal in deciding who wins a procurement award. For example, when Poland purchased the F-16 in 2002, the bidders' offset proposals accounted for only fifteen points out of a total of one hundred.[36] However, because other award criteria, such as price and operational considerations, were closely matched, offsets became a key deciding factor in the procurement.[37] Offsets frequently prove to be a crucial deciding factor because, in comparison to a defense item's capabilities and price, an offset package is far more flexible and under a vendor's control.[38] Offsets allow defense vendors to fashion creative proposals to win procurement awards,[39] and this quality has led offset advocates to justify them as a persuasive "marketing tool" for defense vendors.[40] If a vendor is unethical, though, the offset marketing may also include bribery.[41]

Market and the Implications for U.S. National Security Policy 51 (2009).

[30] Jacques Gansler, Democracy's Arsenal: Creating A Twenty-First-Century Defense Industry 66, 150-151 (2011).

[31] *Id*. at 32-34, 150, 311.

[32] Lamont & Boxell, *supra* note 28, at 7.

[33] *See* Taylor, *supra* note 29, at 31.

[34] E. Anders Eriksson et al., S*tudy on the Effects of Offsets on the Development of a European Defence Industry and Market* 30 (2007); *see also* U.S. Dep't Of Commerce, Offsets In Defense Trade: Twelfth Study at Appendix F (2007) (offsets as part of procurement decision) [hereinafter Dep't Of Commerce, Twelfth Study].

[35] Eriksson, *supra* note 35, at 30.

[36] Barre R. Seguin, *Why Did Poland Choose the F-16?*, George C. Marshall European Center For Security Studies Occasional Paper No. 11, at 11, 16 (2007). In the Polish fighter jet procurement, competitors were scored on a 100-point scale, with 45 points for best price, 40 points for tactical and operational criteria, and 15 points for offsets. *Id*.

[37] *Id*. at 11, 30-31. Other key deciding factors were the formation of a strategic political and military alliance with the U.S., and financial inducements. *Id*. at 16, 25.

[38] Alon Redlich & Maison Miscavage, *The Business Of Offset: A Practitioner's Perspective, in* The Economics Of Offsets: Defence Procurement And Countertrade 381, 393 (Stephen Martin ed., 1996).

[39] *Id*.

[40] *Foreign Military Sales and Offsets*, *supra* note 18, at 3; Dumas, *supra* note 17, at 16.

[41] Transparency Int'l, Defence Offsets, *supra* note 11, at 14.

High-level negotiations are still another factor contributing to offsets' vulnerability to corruption. Traditionally, negotiations have been disfavored in government procurements due to the perception that they are vulnerable to unjust favoritism, collusion, and fraud, as well as being a means of enabling covert bribe payments.[42] In defense offsets, this traditional unease about negotiations has merit[43] because local politicians in the past have inserted themselves into offset negotiations.[44] During the Polish F-16 negotiations, for example, the Polish offices of the President and Prime Minister interjected themselves into negotiations to promote favorite offset projects and to seek assurances their political districts would be offset beneficiaries.[45] This situation is a textbook example of a transaction with high corruption risk.[46] This risk is further exacerbated by the fact that many top purchasers of defense equipment and offsets are located in regions dealing with significant corruption.[47]

Finally, offsets are vulnerable to corruption because they often involve transactions unrelated to the work of the main defense sale. According to the Department of Commerce, forty percent of offsets, as measured by actual value, are "direct" offsets, meaning they relate directly to the defense article or service purchased.[48] Direct offsets usually require the manufacture of a weapon or its components in the purchaser's country, and are concentrated in aerospace-related industries.[49] In contrast, fifty-nine percent of offsets, as measured by actual value, are "indirect" offsets, meaning they are unrelated to the defense article or service purchased.[50] Indirect offsets are diffused among a wide variety of industries such as motor vehicle parts, mining machinery, industrial chemicals, machine tools, wine

---

[42] Steven Feldman, Government Contract Awards § 2:4 (2011) (discussing corruption in negotiations in general).

[43] Ernst & Young, Growing Beyond: A Place for Integrity 19 (12th Global Fraud Survey 2012) (negotiations as leading to corruption in offset agreements).

[44] Transparency Int'l, Defence Offsets, *supra* note 11, at 19.

[45] Seguin, *supra* note 37, at 24.

[46] Brian Loughman & Richard Sibery, Bribery and Corruption: Navigating the Global Risks 297 (2011).

[47] The top seven countries that U.S. defense firms export to are Australia, Egypt, Israel, Japan, South Korea, United Arab Emirates, and the United Kingdom. U.S. Gov't Accountability Office, GAO-10-952, Defense Exports: Reporting on Exported Articles and Services Needs to be Improved 8 (2010) [hereinafter Gov't Accountability Office, GAO-10-952]. Of these countries, Transparency International ranked Egypt as 112 out of 182 countries for the cleanliness of its government, and the Middle East was ranked as the second-most corrupt region in the world after Sub-Saharan Africa. Transparency Int'l, Corruption Perceptions Index 2011 at 6-9 (2011) [hereinafter Transparency Int'l, Corruption Perceptions Index].

[48] Dep't of Commerce, Sixteenth Study, *supra* note 10, at 5, 27.

[49] *Foreign Military Sales and Offsets, supra* note 18, at 4; Ann Markusen, *Arms Trade As Illiberal Trade, in* Arms Trade And Economic Development 66, 75 (Jurgen Brauer & J. Paul Dunne eds., 2004).

[50] Dep't of Commerce, Sixteenth Study, *supra* note 10, at 5, 27.

and food products, and computer software.[51] The categorization of an offset as direct or indirect can be difficult, especially if it involves technology such as aerospace software that may be applied to both civilian and military sectors.[52] One European study estimated that twenty-five percent of European defense offset transactions are completely unrelated to the defense industry.[53] For example, in the 1980s, the F-18 sale to Spain involved indirect offsets promoting tourism,[54] and in the 1990s, Greek indirect offsets financed investments in medical diagnostics, sportswear manufacture, and financial services software.[55] Such deals prompt questions about whether they serve the purchasing government's interests, or ulterior, improper interests.[56]

B. Disparate Policy Goals

Another reason offsets are susceptible to corruption is their disparate policy goals. Purchasing governments use offsets to promote multiple national security and economic development interests, and this combination of disparate policy goals can make it difficult for third parties to discern a particular offset's purpose, or monitor its success.[57]

The primary reason that purchasing governments require defense offsets is to mitigate national security concerns. When a government purchases a foreign weapon, typically it is because its domestic defense industries are incapable of manufacturing the weapon on their own.[58] However, if a purchasing government

---

[51] Markusen, *supra* note 50, at 75.

[52] Aris Georgopoulos, *Revisiting Offset Practices in European Defence Procurement: The European Defence Agency's Code of Conduct on Offsets*, 20 Pub. Procurement L. Rev. 3, 29 , 33 (2011) [hereinafter Georgopoulos, *Revisiting*].

[53] Eriksson, *supra* note 35, at 3, 23.

[54] *Foreign Military Sales and Offsets, supra* note 18, at 4.

[55] *Concerns Over Offsets Generated Using U.S. Foreign Military Financing Program Funds: Hearing Before the H. Subcomm. on Commerce, Consumer Protection, and Competitiveness, Comm. on Energy and Commerce*, 112th Cong. 4 (1994) (statement of Frank C. Conahan, Assistant Comptroller General, National Security and International Affairs Division).

[56] *See* Transparency Int'l, Defence Offsets, *supra* note 11, at 14-15.

[57] Stefan Markowski & Peter Hall, *Mandatory Defense Offsets—Conceptual Foundations, in* Arms Trade And Economic Development 44, 45 (Jurgen Brauer & J. Paul Dunne eds., 2004) (discussing a lack of clarity in offset objectives).

[58] Bialos, *supra* note 30, at 79. The foreign sources a government may choose from are, 1) purchases from a sole foreign vendor, or 2) purchases from a cooperative, multinational weapons development program, such as the European consortium that developed the Eurofighter Typhoon fighter jet. *Id*. at 79; Jay Edwards, *The EU Defence and Security Procurement Directive: A Step Towards Affordability?*, International Security Programme Paper, 2011/05, 6 (August 2011). In multinational arrangements, governments protect their security of supply interests through the principle of fair return on investment, or "juste retour," which requires weapons programs to allocate the economic value of a project's work to companies in proportion to the financial contributions that those companies' participating governments made to the program. *Commission Green Paper on Defence Procurement*, at 4, 9, COM (2004) 608 final (Sep. 23, 2004) [hereinafter *Green Paper*]; Baudouin Heuninckx, *A Primer To Collaborative Defence Procurement In Europe: Troubles,*

buys a superior foreign weapon, this introduces the risk that an external circumstance such as war, embargo, alliance shifts , or a supply chain disruption could endanger the purchasing government's security of weapon supply.[59] Additionally, a purchasing government could be placed at risk if a foreign vendor's government deprives the purchaser of control over the weapon's technology.[60] To mitigate these risks, purchasing governments require foreign vendors to provide offsets that produce a specified number of weapon components within the purchasing country, and transfer weapon technology to domestic companies.[61]

Governments do not just mandate offsets for national security concerns, they also mandate them for political and economic reasons.[62] By mandating direct offset work to domestic companies, governments ensure domestic defense industries maintain work, and domestic workers stay employed.[63] Additionally, governments require indirect offsets to assist civilian industries through the introduction of fresh capital flows, new technology, and new markets.[64] Overall, offsets allow governments to stimulate industrial development with increased government procurement spending.[65]

Purchasing governments demand offsets to promote various economic and national security policies, and use offsets not only to buy weapons, but also to procure a comprehensive bundle of goods and services that enhance the overall national

---

Achievements And Prospects, 17 Pub. Procurement L. Rev. 3, 123, at 135 (2008). However, *juste retour* and the differing legal problems that it raises is beyond the scope of this thesis.

[59] Baudouin Heuninckx, T*he EU Defence and Security Procurement Directive: Trick or Treat?,* 20 Pub. Procurement L. Rev., 1, 9, at 22 (2011) [hereinafter Heuninckx, *Procurement Directive*].

[60] For example, the European companies developing the F-35 in collaboration with Lockheed Martin will, allegedly at the direction of the U.S. government, receive versions of the F-35 that have protective measures installed in them that will prevent European partners from accessing the F-35's software, understanding its workings, modifying it, or performing repairs. Michele Nones et al., *Europe and the F-35 Joint Strike Fighter (JSF) Program*, Quaderni IAI (English Series), at 59-60 (Gregori Alegi trans., July 2009). *See also* Bialos, *supra* note 30, at 5, 33 (stating that governments traditionally procure defense items from domestic industry to promote technological superiority of their weapons systems).

[61] *Green Paper, supra* note 59, at 4-5 (stating that offset requirements address security of supply and technological superiority concerns); U.S. Gen. Accounting Office, GAO-04-954T, Defense Trade: Issues Concerning the Use of Offsets in International Defense Sales 3 (2004) [hereinafter Gen. Accounting Office, GAO-04-954T] (describing offset requirements set by national laws or policies); Markowski & Hall, *supra* note 58, at 45-46 (stating that offsets use local content requirements to source a portion of the contract value in the buyer's territory); Markusen, *supra* note 50, at 68 (identifying that transfer of technology is typical in offset packages).

[62] Markusen, *supra* note 50, at 85; *see also* Taylor, *supra* note 29, at 31 (citing multiple objectives of offsets to include technology transfer, supporting domestic industry, gaining access to new markets, generating exports, and forming alliances with multinational corporations).

[63] Dumas, *supra* note 17, at 25; Markowski & Hall, *supra* note 58, at 45-46.

[64] Dumas, *supra* note 17, at 25.

[65] Markusen, *supra* note 50, at 80; Dumas, *supra* note 17, at 16.

welfare.[66] However, offsets' multiple goals make it difficult for outside parties such as academians, good government advocates, and ordinary citizens to determine whether a particular offset's goal is national security, economic development, or a combination of both.[67] Without clarity in an offset's policy goal, it becomes difficult for outside parties to measure the offset's success and legitimacy.[68]

C. Complex and Opaque Transactions

A fundamental reason offsets are vulnerable to corruption is because they combine a highly valuable asset with a lack of transparency.[69] Offsets, like defense procurements in general, lack transparency because their negotiation and award are shielded from public scrutiny based on alleged national security concerns.[70] Additionally, because offsets engage in unique, complex transactions and accounting practices, they are difficult to monitor.[71] As a result, parties to an offset may feel emboldened to exploit offsets for corrupt motives.[72]

Defense procurements are subject to secrecy because they involve purchasing items containing national security sensitivity, classified information, and protected commercial information.[73] No government engaging in offsets publishes the terms of individual offset arrangements.[74] Instead, governments publish broad trends

---

[66] Jurgen Brauer, *Economic Aspects of Arms Trade Offsets, in* Arms Trade and Economic Development 54, 55 (Jurgen Brauer & Paul Dunne eds., 2004).

[67] Markowski & Hall, *supra* note 58, at 45 (identifying a lack of clarity in offset objectives).

[68] *See Id*. (showing a difficulty in measuring offset success).

[69] Antoine Boessenkool, *Small Firm, Big Player*, Defense News, June 14, 2010, at 50.

[70] Transparency Int'l, Defence Offsets, *supra* note 11, at 14, 16.

[71] *See* Markowski & Hall, *supra* note 58, at 46 (describing offsets' use of countertrade, local content requirements, and bundled requirements); U.S. Dep't of Def., DoD 5105.38-M, Security Assistance Management Manual, para. C.6.3.9.1 (3 Oct. 2003) (discussing offset costs hidden in contract line items) [hereinafter DoD 5105.38-M].

[72] *See* Organization for Economic Cooperation and Development, Bribery in Public Procurement: Methods, Actors and Counter-Measures 28 (2007) [hereinafter OECD Bribery in Public Procurement] (identifying that a lack of transparency caused by national security concerns and unique procurement requirements makes arms sales vulnerable to corruption).

[73] *See* Directive 2009/81/EC, of the European Parliament and of the Council of 13 July 2009 on the Coordination of Procedures for the Award of Certain Works Contracts, Supply Contracts and Service Contracts by Contracting Authorities or Entities in the Fields of Defence and Security, and Amending Directives 2004/17/EC and 2004/18/EC, 2009 O.J. (L216) 80 at ¶27, 94 at Arts. 13(a) & 13(b) [hereinafter 2009 Directive] (discussing the exclusion of contracts for intelligence activities and contracts containing sensitive information from the E.U. Defense Procurement Directive due to national security and confidentiality concerns); Transparency Int'l, Defence Offsets, *supra* note 11, at 14, 16 (showing the opaque nature of defense procurement); Andrew Feinstein, The Shadow World: Inside the Global Arms Trade 179 (2011) (reviewing offsets hindered by commercial confidentiality).

[74] *See* Martin, *supra* note 7, at 15, 31 (detailing individual offset projects not available in public databases).

about offsets.[75] As a result, offset data is scarce and monitoring offsets is difficult.[76] Moreover, it is difficult to decipher the reported offset information due to offsets' unique terminology, and complex transactions and accounting rules.

First, offsets engage in a complex web of transactions with their own terminology. These transactions fit into three categories: transfers of technology or financing, local content requirements, and countertrade.[77] Because a successful offset package combines several types of transactions,[78] it is important to understand how these types fit together.

Transfers of technology or financing ("transfers") require a vendor to provide an additional product to a purchaser in order to win the main defense sale.[79] These additional products include transferring technology to a company domestic to the purchasing country;[80] training a domestic company on how to produce, maintain, or engineer a product;[81] or lending credit assistance to finance an offset.[82] Transfers provide the technology, practical experience, and financing to start up an offset. The most prevalent type of transfer, technology transfer, made up $10.4 billion (or eighteen percent) of U.S. defense firm offset transactions between 1993 and 2010.[83]

A local content requirement mandates a vendor produce an agreed-upon portion of the contract's value in the purchasing country.[84] For example, a local content requirement may mandate a domestic company of the purchasing country manufacture a fighter aircraft's landing gear.[85] Within local content requirements,

[75] *Id*. at 33.

[76] *Id*.; Eriksson, *supra* note 35, at 3; Bialos, *supra* note 30, at 96.

[77] Markowski & Hall, *supra* note 58, at 45-46.

[78] Markusen, *supra* note 50, at 68.

[79] Markowski & Hall, *supra* note 58, at 46.

[80] Technology transfer may take the form of research and development conducted abroad, technical assistance provided to the subsidiary or joint venture of overseas investment, or other activities under direct commercial arrangement between the defense vendor and offset recipient. Dep't of Commerce, Sixteenth Study, *supra* note 10, at 29.

[81] Training generally includes skills related to the production or maintenance of the exported defense item. Training may also be required in areas unrelated to the defense item, such as computer training, foreign language skills, or engineering capabilities. *Id*.

[82] Credit assistance consists of direct loans, brokered loans, loan guarantees, assistance in achieving favorable payment terms, credit extensions, and lower interest rates. *Id*. at 27.

[83] *Id*. at 22.

[84] Markowski & Hall, *supra* note 58, at 46.

[85] Markusen, *supra* note 50, at 73.

there are four types of trade: subcontracting,[86] licensed production,[87] co-production,[88] and investment.[89] The main distinction between these forms is the transactional format used to package local production. The most prevalent type of local content requirement, subcontracting, made up $11.9 billion (or twenty-one percent) of U.S. defense firm offset transactions between 1993 and 2010.[90]

Countertrade is a reciprocal purchase of goods and services between a defense vendor and purchasing government.[91] Countertrade consists of three specialized types of trade: barter,[92] counter-purchase,[93] and buy-back.[94] A typical barter transaction requires a purchasing government to pay for defense items with raw materials, such as when Iraq paid France for military supplies with oil.[95] A counter-purchase requires a vendor to market and sell manufactured material produced in the purchasing country, such as when a U.S. defense vendor marketed Finnish papermaking machinery in the U.S.[96] Finally, buy-back requires a vendor to invest in a physical plant in the purchasing country, and then buy back a certain portion of the output produced there.[97] The most prevalent type of countertrade, counter-purchase, made up $20.6 billion (or thirty-six percent) of U.S. defense firm offset transactions between 1993 and 2010.[98]

---

[86] Subcontracting is a direct commercial arrangement between the defense prime contractor and a foreign producer to make in the purchasing country a part or component of a US-origin defense article. Dep't of Commerce, Sixteenth Study, *supra* note 10, at 29.

[87] Licensed production is a transfer of technical information under direct commercial arrangements between a manufacturing vendor and a foreign government or producer, made in order to produce in the purchasing country a part or component of a US-origin defense article. *Id*. at 28.

[88] Co-production is a government-to-government agreement authorizing the transfer of technology to permit foreign companies to manufacture all or part of a US-origin defense article. *Id*. at 27. Co-production is made pursuant to a Foreign Military Sale. *Id*.

[89] Investment is a dedication of capital to the establishment of a foreign entity unrelated to the defense sale, or to expanding the US firm's subsidiary or joint venture in the foreign country. *Id*. at 28.

[90] *Id*. at 22.

[91] Markowski & Hall, *supra* note 58, at 46.

[92] Barter is a one-time transfer under a single contract that specifies the exchange of goods or services of equivalent value. Martin, *supra* note 7, at 32.

[93] Counter-purchase is an agreement by the defense vendor to buy, or find a buyer for, a specified value of off-the-shelf items from the offset recipient. *Id*.; Dep't of Commerce, Sixteenth Study, *supra* note 10, at 29.

[94] Buy-back is an agreement for the defense vendor to accept as full or partial repayment products that are derived from the original exported product. Martin, *supra* note 7, at 32.

[95] Jean-Paul Hebert Interdisciplinary Research Center For Peace And Strategy Surveys-Paris, *Offsets And French Arms Exports, in* The Economics Of Offsets: Defense Procurement And Countertrade 139, 141-142 (Stephen Martin, ed. 1996).

[96] Brauer, *supra* note 67, at 56-57.

[97] *Id*. at 55.

[98] Dep't of Commerce, Sixteenth Study, *supra* note 10, at 22.

Second, in addition to unique terminology, unique accounting practices add an extra layer of complexity to offset transactions. These accounting practices affect both the selection and discharge of a procurement. During the selection phase, an offset proposal may be scored in terms of its cost, or an estimated value based on speculative, indefinite, or arbitrary formulas.[99] During the discharge phase, an offset may be satisfied by a vendor earning offset credit, and not by completing performance.[100] Both of these practices are made possible by five unique offset accounting practices.

The first accounting practice is that offset agreements specify the level of offset activity required by expressing it as a percentage of the contract's purchase price.[101] For example, a purchasing government may require a beginning bid for a defense contract to contain at least thirty percent of its value as offset activity.[102] Many countries require an offset's value to be one hundred percent or more of a contract's purchase price.[103]

For an offset to be worth more than the contract it is attached to, the second oddity of offset accounting must exist. Purchasing governments must use multipliers to grant additional offset credit to activities they wish to encourage.[104] A multiplier is a number that is compounded with the actual value of an offset transaction in order to calculate a higher or lower credit value.[105] A multiplier may increase an activity's credit value by a factor of two, ten, or even thirty.[106] Offset guidelines will state what multiplier a government will assign to specific types of offset activity.[107]

---

[99] *See* Transparency Int'l, Defence Offsets, *supra* note 11, at 17 (criticism of offset valuation criteria); The U. N. Comm'n on On Int'l Trade Law, Legal Guide on International Countertrade Transactions 67-68, 71-72 (1993) [hereinafter UNCITRAL Legal Guide] (providing various methods for calculating the value of an offset); Dep't of Commerce, Sixteenth Study, *supra* note 10, at 27; Feinstein, *supra* note 74, at 177-178 (discussing South African procurement scoring offsets based on their assessed value); Won-Joon Jang et al., *The Defense Offset Valuation Model*, The DISAM Journal, Dec. 2007, at 91, 92-93 (discussing the Korean government assessing technology offsets based on valuation models, as opposed to assessments based on cost).

[100] *See* Gen. Accounting Office, GAO/NSIAD-96-65, *supra* note 10, at 2 (offset credits as satisfying performance); Eriksson, *supra* note 35, at 30 (banked offset credits as satisfying performance); Barry Marvel, *The Reverse Piggyback Offset*, Contract Management, Jul. 1, 2001 at 36 (banked offset credits as satisfying performance).

[101] Gen. Accounting Office, GAO/NSIAD-96-65, *supra* note 10, at 2.

[102] *Id*. at 27-28 (discussing the minimum offset percentage for Korean defense contracts above $5 million in late 1980s).

[103] Eriksson, *supra* note 35, at 30; *see also* Dep't Of Commerce, Twelfth Study, *supra* note 35, at Appendix F.

[104] Gen. Accounting Office, GAO/NSIAD-96-65, *supra* note 10, at 2; Gen. Accounting Office, GAO-04-954T, *supra* note 62, at 1; Ron Matthews, *Defense Offsets: Policy Versus Pragmatism, in* Arms Trade And Economic Development 89, 98 (Jurgen Brauer & J. Paul Dunne eds., 2004).

[105] Dep't of Commerce, Sixteenth Study, *supra* note 10, at 28.

[106] *See* Dep't Of Commerce, Twelfth Study, *supra* note 35, at Appendix F (showing offset multipliers used by Greece, the Netherlands, and Taiwan).

[107] Redlich & Miscavage, *supra* note 35, at 395-396.

Some offset policies allow government officials to assign a range of multipliers to offset activity. For example, the value for a research and development proposal may be multiplied anywhere from one hundred to two hundred percent of its actual value in a Middle Eastern country, and may be multiplied by a factor of just ten to thirty in a European country.[108]

The third accounting practice is to base an offset's credit value at award on cost, or on a formula devised by the purchaser.[109] Valuing an offset at cost may be inappropriate because, for example, a defense vendor transferring its technology to a local company may demand the purchasing government compensate it for future royalties generated by the transfer.[110] However, valuation is a major weak point in offsets because market data may be unavailable for the offset's subject, or because there may be imperfect data about the production abilities of an offset recipient.[111] To value future royalties, governments fix a value in reference to projected production, sales, or profits, but such benefits may fail to materialize during performance.[112]

The fourth accounting practice is to require a vendor to earn a specified number of offset credits which are earned by engaging in activities listed in the offset agreement.[113] For example, to earn the required number of offset credits, a vendor must sell a certain number of products in countertrade.[114] To obtain discharge, a vendor must present its offset activity to an official in the purchasing government who determines whether the activity actually earned the required number of credits.[115]

The final accounting practice is to allow a vendor to "bank" excess credits earned or to sell excess credits to other vendors.[116] For example, if a vendor sells more products in countertrade than required, it can store this extra value as banked

---

[108] *Id*. at 395; Dep't Of Commerce, Twelfth Study, *supra* note 35, at Appendix F.

[109] *See* Jang et al., *supra* note 100, at 92-93 (describing technology valuation models to assess offset proposals, as opposed to assessments based on cost).

[110] *See* UNCITRAL Legal Guide, *supra* note 100, at 71-72.

[111] James C. Nobles, Jr. & Johannes Lang, T*he UNCITRAL Legal Guide on International Countertrade Transactions: The Foundation for a New Era in Countertrade?*, 30 Int'l Law 739, 749 (1996) (offset valuation as a weak point); Gen. Accounting Office, GAO/NSIAD-96-65, *supra* note 10, at 2 (lack of market data); Markowski & Hall, *supra* note 58, at 47, 49 (lack of market data and imperfect data on merits of a local contractor).

[112] *See* UNCITRAL Legal Guide, *supra* note 100, at 72 (showing valuation methods for offset royalties); Markowski & Hall, *supra* note 58, at 49 (providing the risk of default on offset obligations); Dumas, *supra* note 17, at 22 (citing a risk of vendors shirking offset obligations or performing them in a perfunctory manner).

[113] Gen. Accounting Office, GAO/NSIAD-96-65, *supra* note 10, at 2.

[114] Markowski & Hall, *supra* note 58, at 46.

[115] Gen. Accounting Office, GAO/NSIAD-96-65, *supra* note 10, at 2.

[116] Eriksson, *supra* note 34, at 30; Marvel, *supra* note 101, at 36; Sandeep Verma, *Offset Contracts Under Defence Procurement Regulations in India: Evolution, Challenges and Prospects* 25, (H.C.M. Rajasthan State Institute of Public Administration Occasional Paper No. 16, 2009) *available at* http://ssrn.com/abstract=1464709.

offset credits. Banked offset credits mitigate the risk of defaulting on an offset obligation because in lieu of default, a vendor may cash in or purchase banked offset credits.[117]

The potential for these accounting practices to frustrate transparency and invite corruption is apparent in a South African offset arrangement connected to the purchase of German submarines. In this arrangement, the offset requirement was in excess of four hundred percent of the contract price.[118] It is unclear how an offset, which is supposed to recoup part of the purchase price,[119] could be worth four times the value of the item purchased. Such a valuation seems disingenuous, but it is the current state of affairs in offset practice.

D. Third Party Agents

The hire of third party agents and consultants is the final factor making offsets vulnerable to corruption. Foreign agents and consultants create a significant corruption risk due to their personal ties to high-ranking officials in their countries' defense ministries, and due to their own compromised ethical standards.[120] This risk is evidenced by their involvement in more than ninety percent of reported FCPA cases.[121] Yet despite this risk, many vendors hire third parties to develop and deliver offset packages.

Defense vendors hire agents and consultants mainly to develop and deliver indirect offset projects that are beyond the vendors' areas of expertise.[122] To manage direct offset packages, many defense vendors establish separate in-house operations.[123] In the offer stage, an offset agent assists a vendor by developing multiple indirect offset proposals that correlate to the vendor's strengths and the purchasing country's needs.[124] To develop these proposals, agents employ think tanks consisting of high level ex-government, military, and industry leaders, as well as field representatives and proposal evaluators.[125] In the performance stage,

---

[117] Marvel, *supra* note 101, at 36.

[118] Matthews, *supra* note 105, at 98.

[119] *See* Brauer & Dunne, *supra* note 13, at 3 (citing Udis & Maskus, *supra* note 13 at 152 (discussing how offsets allow purchasing governments to recoup, or offset, some of their investment).

[120] Loughman & Sibery, *supra* note 47, at 299; Interview with Lorrine L. Romero, Senior Counsel, General Law, Raytheon, in Arlington, VA (Mar. 8, 2012); Marvel, *supra* note 101, at 36.

[121] APCO Oil & Gas Int'l, Inc., FCPA Guide, http://www.apcooilandgas.com/profiles/investor/FullPage.asp?BzID=1671&ID=9892&secid=0, (last visited May 17, 2012); Loughman & Sibery, *supra* note 47, at 96. For a discussion of the FCPA, *see infra*, Section IV of this thesis.

[122] Markusen, *supra* note 50, at 77; Redlich & Miscavage, *supra* note 35, at 393; Woolf Committee Report, *Business Ethics, Global Companies And The Defense Industry* 25, 28 (2008).

[123] Markusen, *supra* note 50, at 71.

[124] Redlich & Miscavage, *supra* note 39, at 381, 385.

[125] *Id*. at 398.

an agent may perform an offset on behalf of a vendor.[126] In such a capacity, offset agents may purchase and resell offset goods like a trading company, or market offset goods for purchase by other parties.[127] In exchange for their services, agents may charge a fee calculated as a fixed price per unit of goods sold, or as a percentage of the offset item's purchase price.[128]

The corruption risk posed by agents is present in every offset stage. During the offer stage, the potential political power of think tank members may create conflicts of interest that compromise an agent's offset proposals.[129] There is also a danger that agents may place the pet projects of government officials into their proposals without properly vetting them.[130] In the performance stage, agents may sell offset goods with the aid of corrupt payments, either with or without the knowledge of thedefense vendor.[131] Offset agents being paid on commission exacerbate these risks.[132]

Despite concerns about agents' corruption, the burden of creating and satisfying offset proposals is so substantial that defense vendors and governmental authorities now accept offset proposals sold to them by third party companies.[133] These proposals, called "reverse piggyback offsets," originate from companies entirely independent of the defense vendor and purchasing government.[134] Accepting a reverse piggyback offset is even riskier than accepting normal agent proposals, yet the pressure or desperation to create and fulfill offsets has made it possible for such risky offset practices to exist.[135]

---

[126] Redlich & Miscavage, *supra* note 39, at 381; Woolf Committee Report, *supra* note 123, at 28.

[127] UNCITRAL Legal Guide, *supra* note 100, at 78 (showing offset third parties acting as trading companies); Redlich & Miscavage, *supra* note 39, at 385 (showing offset brokers as marketers for a targeted country).

[128] UNCITRAL Legal Guide, *supra* note 100, at 85.

[129] Marvel, *supra* note 101, at 36.

[130] Romero, *supra* note 121.

[131] Woolf Committee Report, *supra* note 123, at 25, 28 (2008).

[132] *Id*.

[133] Marvel, *supra* note 101, at 36.

[134] *Id*. The "reverse" term refers to the broker seeking out the multi-national corporation with an offset proposal, versus the corporation hiring the broker to then develop a proposal. The "piggyback" term refers to the broker piggybacking its own offset project onto the corporation's sponsorship into a foreign market.

[135] *See* Markusen, *supra* note 50, at 77 (vendors buying offset credits in the market from brokers).

III. MAJOR INTERNATIONAL OFFSET REGULATIONS

Although international trade in defense offsets generates billions of dollars in revenue, a remarkable aspect of offset trade is how lightly it is regulated.[136] Defense procurement offsets face no substantial WTO regulation, which leaves purchasing and exporting countries with a free hand. This has led to a divide in how governments regulate offsets. The European Union attempting to restrict them, while the United States has left them largely unregulated.

A. Agreement on Government Procurement

The WTO's Agreement on Government Procurement (GPA)[137] expressly prohibits acceding countries from imposing, seeking, or considering offsets.[138] However, the GPA's offset prohibition does not stop GPA members from demanding offsets in their defense procurements.[139] This dissonance occurs because the GPA's offset prohibition contains two exceptions utilized for defense procurements.

First, GPA Article XXIII states its terms do not apply either to procurements for "arms, ammunition or war materials" or to procurements "indispensable for national security," if the acceding nation considers either type of procurement "necessary for the protection of its essential security interests."[140]

Second, the GPA covers a defense ministry's procurement of non-armament items only if the country has negotiated an inclusion for them, as reflected in that country's individual GPA annex.[141] The terms of a country's annex can exclude GPA coverage of a defense ministry purchase if the purchase falls below a certain

---

[136] Gen. Accounting Office, GAO-04-954T, *supra* note 62, at 2 (identifying offsets unregulated in U.S.); Eriksson, *supra* note 35, at 29 (identifying offsets regulated by only half of members of the E.U., and existing regulations in some countries are non-binding); Dep't of Commerce, Sixteenth Study, *supra* note 10, at 4 (providing offsets entered into by U.S. companies generating $56 billion in trade between 1993 and 2010).

[137] Revision of the Text of the 1994 Agreement on Government Procurement, Marrakesh Agreement Establishing the World Trade Organization, Annex 4, (Dec. 15, 2011) [hereinafter GPA]. The GPA establishes an international framework of rights and obligations regarding government procurement. The cornerstone principles of the GPA are non-discrimination and transparency in government procurement among its member states. Because the GPA is a "plurilateral" agreement, only WTO members who are signatories to the GPA are bound by its terms. *See* World Trade Organization, *Government Procurement: The Plurilateral Agreement, available at* http://www.wto.org/english/tratop_e/gproc_e/ gpa_overview_e.htm.

[138] GPA, *supra* note 138, at art. XVI(1).

[139] For example, although the E.U. is a member of the GPA, many E.U. member states still have laws or policies requiring offsets for their defense procurements. *Id*. at E.U. Annex 1 (identifying E.U. membership in the GPA); Eriksson, *supra* note 35, at 4 (providing offset policies of a sample of E.U. member states).

[140] GPA, *supra* note 138, at art. XXIII(1).

[141] In the U.S. Annex to the GPA, for example, multiple types of purchases are explicitly excluded from GPA coverage. GPA, *supra* note 138, at U.S. Annex 1.

dollar threshold, or if the purchase is made by an agency within the defense ministry that is explicitly excluded from GPA coverage.[142] Additionally, a defense ministry purchase can be excluded if a country's annex states such a purchase is covered only if its subject is specifically included on a list in the annex.[143] In this situation, a country may strategically fail to list certain types of goods or services.[144]

Both of these exceptions work together to exclude defense offsets from GPA restrictions. For example, Japanese defense aircraft procurements have required an indirect offset for automobile parts manufacturing.[145] The GPA's offset prohibition does not apply for two reasons. First, a defense ministry is purchasing the offset through an armament procurement.[146] Second, the offset is for an automotive product, which is not listed as a covered defense ministry item in Japan's GPA Annex.[147] Therefore, Japan has successfully and legally required automotive defense offsets.

B. European Union Regulations

The European Union disfavors offsets and has initiated two recent efforts to curb their use: a voluntary Code of Conduct on Offsets, and an E.U. Defense Procurement Directive. However, like the WTO, the European Union's efforts do not effectively regulate defense offsets.

E.U. Member States control their own defense procurements, and as a result, E.U. defense procurements have historically been fragmented along national lines.[148] Similarly, the European Union has fragmented offset rules, with about half the member states requiring offsets through laws, decrees, or ministerial regulations.[149] Although the European Defence Agency (EDA) is not in favor of defense offsets,[150] the European Union has not banned offsets outright due to their politically sensitive nature.[151]

---

[142] Arie Reich, *The New Text of the Agreement on Government Procurement: An Analysis and Assessment*, 12 J. Int'l Econ. L. 989, 992 (2009).

[143] *Id*.

[144] *Id*.

[145] Markusen, *supra* note 50, at 76.

[146] Although an offset may be managed in some countries by a separate ministry, the purchase of the offset itself is done through the defense ministry. *See* Marvel, *supra* note 101, at 36.

[147] GPA, *supra* note 138, at Japan Annex 1; Markusen, *supra* note 50, at 76 (auto parts offsets in Japan).

[148] Stacy N. Ferraro, T*he European Defence Agency: Facilitating Defense Reform or Forming Fortress Europe?*, 16 Transnat'l L. & Contemp. Probs. 549, 555 (2007); Green Paper, *supra* note 59, at 4.

[149] Eriksson, *supra* note 35, at 29.

[150] *Id*. at 25 (discussing an EDA study opining offsets violate the free movement of goods and services required by the European Community Treaty); Georgopoulos, *Revisiting, supra* note 53, at 31.

[151] Georgopoulos, *Revisiting, supra* note 53, at 30, 31.

Instead of banning offsets, in 2011 the European Union promulgated a voluntary Code of Conduct which recommends basic offset agreement principles.[152] These principles include clearly stipulating offset requirements in contract notices, minimizing the weight of offsets as award criteria, and not having offset valuation exceed the value of the procurement contract.[153] The goal of these principles is to mitigate the adverse effects of offsets.[154] However, it has not appreciably affected E.U. offset practices because it has no enforcement mechanism.[155]

The second E.U. effort to restrict offsets is the 2009 defense procurement regulation, Directive 2009/81/EC ("Directive").[156] Like the GPA, the Directive states a general rule that contracting authorities must treat all bidders for defense procurements in a non-discriminatory manner.[157] This rule probably prohibits discrimination in defense offsets, even though the Directive does not mention offsets.[158] Although the Directive's rules apply to all military equipment procurements(i.e., "equipment specifically designed or adapted for military purposes and intended for use as an arm, munitions or war material"),[159] its terms do not restrict offset practice in a meaningful way. Specifically, the Directive's terms do not cover cooperative development program procurements;[160] international agreements or arrangements, such as Memoranda of Understanding (MOUs);[161] and government-to-government contracts.[162] These exceptions swallow the Directive's rule against non-discrimination, because they exclude all the current E.U. defense procurement mechanisms. Using aircraft as an example, E.U. Member States currently use collaborative procurement for the Eurofighter Typhoon,[163] an MOU for the F-35,[164] and a government-to-government sale for the F-16.[165] As a result, the Directive's anti-discrimination rules are toothless for offsets connected to these procurements.

---

[152] European Defence Agency, *Code of Conduct on Offsets* 1 (last visited May 3, 2011), *available at* http://www.eda.europa.eu/migrate-pages/Otheractivities/CoCOffsets.

[153] *Id*. at 3-4.

[154] *Id*. at 1.

[155] *See* Georgopoulos, *Revisiting, supra* note 53, at 32 (identifying a lack of enforcement mechanism in Code of Conduct on Offsets).

[156] 2009 Directive, *supra* note 74, at 76.

[157] GPA, *supra* note 138, at art. III; 2009 Directive, *supra* note 74, at 92.

[158] Heuninckx, *Procurement Directive, supra* note 60, at 25-26.

[159] 2009 Directive, *supra* note 74, at 90-91.

[160] *Id*. at art. 13(c), 2009 O.J. (L216) 76, 94.

[161] *Id*. at art. 12, 2009 O.J. (L216) 76, 94; Christopher R. Yukins, Feature Comment, *The European Defense Procurement Directive: An American Perspective*, 51 Gov't Contractor ¶ 383, Nov. 4, 2009, at 6.

[162] 2009 Directive, *supra* note 74, at 94.

[163] Edwards, *supra* note 59, at 6.

[164] Nones, *supra* note 61, at 8-9; U.S. Gen. Accounting Office, GAO-03-775, Joint Strike Fighter Acquisition: Cooperative Program Needs Greater Oversight to Ensure Goals are Met 1 (2003) [hereinafter Gen. Accounting Office, GAO-03-775].

[165] Seguin, *supra* note 37, at 11.

C. United States Regulations

In contrast with the European Union, the United States has a "hands off" approach and does not attempt to directly regulate offsets.[166] The United States maintains that deciding whether to engage in offsets, and the responsibility for negotiating and implementing those offsets, resides with the parties involved.[167] However, the United States does maintain indirect control over offset agreements entered into by U.S. companies.[168] Specifically, the United States restricts offsets through its rules for Direct Commercial Sales (DCS) and Foreign Military Sales (FMS). However, DCS and FMS restrictions are broad and unsophisticated.

When a U.S. vendor sells defense articles, services, or technical data to a foreign government, it must do so through the DCS or FMS programs.[169] DCS are commercial exports to a foreign government authorized under the Arms Export Control Act.[170] Before export, a defense vendor must obtain an export license per the International Traffic in Arms Regulations.[171] DCS are negotiated directly between a defense vendor and purchasing government, and offset provisions may be part of the main contract or a separate agreement.[172] The United States exerts control over potential DCS offsets by not granting an export license for technology requested by a purchasing government. As a result, around eighty-five percent of U.S. offsets are satisfied with technology at least ten years old.[173]

FMS are government-to-government agreements where the Department of Defense (DOD) sells arms to foreign governments.[174] Under FMS, defense vendors do not sell directly to the purchasing governments and do not obtain an export

---

[166] U.S. Gen. Accounting Office, GAO/NSIAD-93-13, Military Exports: Recent Implementation of Offset Legislation 4 (1990); Gen. Accounting Office, GAO-04-954T, *supra* note 62, at 2.

[167] Defense Production Act Amendments of 1992, Pub. L. No. 102-558, Title I, Part C, § 123, 106 Stat. 4198); *see* Udis & Maskus, *supra* note 18, at 359-360 (discussing the refusal of the U.S. government to intervene with a foreign government to satisfy an offset obligation after 1978).

[168] An additional U.S. statutory control of offsets is the Feingold Amendment, which prohibits vendors and their agents from making incentive payments for the satisfaction of offset obligations. 22 U.S.C. § 2779a (2010). For a discussion of the politics behind the creation of this amendment, *see* Udis & Maskus, *supra* note 18, at 366-367.

[169] The Defense Institute of Security Assistance Management, The Management of Security Assistance 1-2, 1-6, 15-1 (27th ed. 2007) [hereinafter DISAM].

[170] *Id.* at 1-6. For the general criteria a defense export must meet to obtain an export license, *see* The Arms Export Control Act, 22 U.S.C. § 2753 (2010).

[171] Foreign Relations Violations, 22 C.F.R. § 127.1(a); DISAM, *supra* note 170, at 15-2.

[172] DISAM, *supra* note 169, at 15-2.

[173] Dep't of Commerce, Sixteenth Study, *supra* note 10, at 14; Matthews, *supra* note 105, at 99 (stating that 85 percent of U.S. offsets were satisfied with technology that is over 10 years old).

[174] United States ex. rel. Campbell v. Lockheed Martin Corp., 282 F. Supp. 2d 1324, 1327 (M.D. Fla. 2003); DISAM, *supra* note 170, at 1-2; *See also* Defense Federal Acquisition regulation supplement [hereinafter DFARS], § 225.7300-7307 (2002) for FAR regulations pertaining to FMS.

license.[175] Instead, the U.S. Government agrees to sell the foreign government the defense item. In turn, the U.S. Government contracts separately with the vendor under the Federal Acquisition Regulation (FAR) to purchase the item for resale to the foreign government.[176]

Offsets become part of FMS exports when a purchasing government first conducts its own procurement competition among several nations' vendors. In this process, a U.S. vendor submits an offset proposal as part of its bid, the purchasing government picks the U.S. vendor's bid, and the purchasing government then approaches the U.S. government to request a sole-source FMS award to its chosen U.S. vendor.[177]

FMS occurs through a contract between the U.S. Government and purchasing government called a Letter of Offer and Acceptance (LOA), but an FMS offset occurs in a separate agreement between the defense vendor and purchasing government.[178] This separate offset arrangement exists because of the U.S. Government's policy to not be a party to offset agreements.[179] However, to recover its offset costs, the defense vendor increases the LOA's sales price.[180] Specifically, the vendor increases the line item unit price of the defense item, and does not account for offset costs separately.[181] As a result, the defense vendor bills the U.S. Government for both the defense item and offset, and the U.S. Government recovers these costs from the purchasing government.[182]

The U.S. Government's regulation of FMS offsets is indirect and broad. Nevertheless, it places some restraint on offset subcontracting and accounting practices. For subcontracting, a DOD contracting officer will honor a purchasing government's request to place a subcontract with a particular firm only if there is full and open competition, or if the LOA specifically requires a product be obtained from this firm.[183] To justify a sole source request, a purchasing government must

---

[175] Foreign-Owned Military Aircraft and Naval Vessels, and the Foreign Military Sales Program, 22 C.F.R. § 126.6; DISAM, *supra* note 169, at 1-2.

[176] *Campbell*, 282 F. Supp. 2d at 1327.

[177] *See* DISAM, *supra* note 169, at 9-7 (describing the availability of sole-source FMS due to a purchasing government's competition); FAR § 6.302-4 (1998) (stating that sole source selection by the U.S. government is allowed when acquisition will be reimbursed by a foreign country through a Letter of Offer and Acceptance); Redlich & Miscavage, *supra* note 39, at 393 (identifying defense item, price and offset package as the three parts of a defense vendor's bid to a purchasing government).

[178] DISAM, *supra* note 169, at 9-7, 9-19 - 9-20.

[179] *Id*. at 9-19 - 9-20; DFARS § 225.7306.

[180] DISAM, *supra* note 169, at 9-19 to 9-20; FAR § 225.7303-2(a)(3) (2012); DoD 5105.38-M, *supra* note 72, at C6.3.9.1.

[181] DISAM, *supra* note 169, at 9-19 to 9-20; DoD 5105.38-M, *supra* note 72, at C6.3.9.1.

[182] *See* DISAM, *supra* note 169, at 9-20 (showing that the U.S. government is the "banker" for offset transactions).

[183] DFARS § 225.7304(a) (2012); FAR § 6.302-4 (1998). "Full and open competition" is when all

provide written rationale to U.S. contracting authorities demonstrating how the sole source is based on the purchasing government's objective needs, and how excluding other sources is not arbitrary, capricious, or discriminatory.[184] For accounting practices, because DOD assumes responsibility for a fair price being paid for an FMS acquisition, a DOD contracting officer must determine whether a vendor's offset costs are reasonable and allocable.[185] Such a determination is usually made by a contract officer's review of an offset's projected labor, material, and overhead costs.[186] This review of offset costs, while not perfect, provides some deterrent to placing illegal charges within an LOA.

IV. MAJOR INTERNATIONAL ANTI-CORRUPTION OFFENSES

Although there is no effective international regulation of offsets, there are several criminal statutes in multiple jurisdictions which punish corrupt conduct in an offset agreement. The most prominent statutes are the U.S. Foreign Corrupt Practices Act (FCPA),[187] the U.K. Bribery Act 2010 (Bribery Act),[188] and the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions (Anti-Bribery Convention).[189] These laws take different approaches to regulating international corruption, but when their disparate provisions are combined, they create four offenses covering defense offset corruption: bribery of a foreign official,[190] commercial bribery,[191] recordkeeping and internal control violations,[192] and failure of a commercial organization to prevent bribery.[193] In addition, because approximately forty percent of U.S. defense export sales (and their

responsible sources are permitted to compete in a contract action. FAR § 2.101 (2013).

[184] DoD 5105.38-M, *supra* note 72, at C6.3.4; Anthony J. Perfilio, Foreign Military Sales Handbook § 6:13 (2010).

[185] Perfilio, *supra* note 185, at §§ 5:3, 5:27. Under the FAR, a cost is reasonable if, in its nature and amount, it does not exceed that which would be incurred by a prudent person in the conduct of competitive business. FAR § 31.201-3 (1998). A cost is allocable if it is assignable or chargeable to a contract. FAR § 31.201-4 (1998).

[186] Interview with Charles Blair, Branch Chief, Aviation Procurement Law Section, Army Aviation Life Cycle Management Command, U.S. Department of the Army (Feb. 24, 2012); *but see* Perfilio, *supra* note 185, at § 5:27 (displaying a contracting officer not having much visibility over offset costs in a competed FMS contract).

[187] 15 U.S.C. §§ 78dd-1 – 78ff, 78m (1998).

[188] Bribery Act, c.23, 2010 (U.K.).

[189] Organisation for Economic Co-operation and Development, Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, Nov. 21, 1997, 37 I.L.M. 1, art. 1 [hereinafter OECD Anti-Bribery Convention].

[190] 15 U.S.C. §§ 78dd-1(a), 78dd-2(a), 78dd-3(a) (1998) (stating that bribery of foreign officials is prohibited by securities issuers, domestic concerns, and persons other than issuers or domestic concerns); Bribery Act, c.23, § 6, 2010 (U.K.) (bribery of a foreign public official); OECD Anti-Bribery Convention, *supra* note 190, at art. 1 (bribery of a foreign public official).

[191] Bribery Act, c.23, § 1, 2010 (U.K.) (bribing another person).

[192] 15 U.S.C. § 78m (1998).

[193] Bribery Act, c.23, § 7, 2010 (U.K.).

accompanying offsets) occur through FMS,[194] U.S. defense vendors face liability under the False Claims Act[195] for corrupt offset transactions.

A. Bribery of a Foreign Official

The FCPA, Bribery Act, and Anti-Bribery Convention each prohibit individuals and corporations from bribing foreign officials.[196] Although these laws generally track with each other in their elements,[197] each uses different phraseology and approaches.[198] More importantly, all three laws create flexible frameworks for punishing bribes of foreign officials, no matter what mechanism a party uses to transfer the bribe.

The general principles criminalizing bribery of a foreign official were created by the Anti-Bribery Convention, which is an international agreement that requires signatory countries to enact laws that implement its anti-bribery provisions.[199] The Anti-Bribery Convention entered into force in 1999. By 2012, forty countries had ratified it.[200] The Anti-Bribery Convention makes it illegal for any person to offer, promise, or give an undue payment to a foreign public official in order to obtain or retain business, or to receive any other improper advantage.[201] An undue payment is

---

[194] Gov't Accountability Office, GAO-10-952, *supra* note 48, at 6-7.

[195] 31 U.S.C. §§ 3729-3733 (2009).

[196] 15 U.S.C. §§ 78dd-1(a), 78dd-2(a), 78dd-3(a) (1998); Bribery Act, 2010, c.23, § 6 (U.K.); OECD Anti-Bribery Convention, *supra* note 190, at art. 1.

[197] Loughman & Sibery, s*upra* note 47, at 12; F. Joseph Warin et al., *The British are Coming!: Britain Changes its Law on Foreign Bribery and Joins the International Fight Against Corruption*, 46 Tex. Int'l L.J. 1, 15 (2010).

[198] *See* 15 U.S.C. §§ 78dd-1(a), -2(a), -3(a); Bribery Act, c.23, § 6, 2010 (U.K.). The OECD does not require uniformity of language among countries' statutes, but only functional equivalence. Organization for Economic Co-operation and Development, Convention on Combating Bribery of Foreign Public Officials in International Business Transactions and Related Documents 14 (2011) [hereinafter OECD Related Documents].

[199] OECD Anti-Bribery Convention, Nov. 21, 1997, 37 I.L.M. 1, preamble, art. 1; Organisation for Economic Cooperation and Development, OECD Anti-Bribery Convention: Entry into Force of the Convention, *available at* http://www.oecd.org/document/12/0,3746, en_2649_34859_2057484_1_1_1_1,00.html (last visited July 18, 2012) [hereinafter OECD Entry Into Force].

[200] OECD Anti-Bribery Convention, Nov. 21, 1997, 37 I.L.M. 1, preamble; OECD Entry Into Force, *supra* note 200. The forty countries are: Argentina, Australia, Austria, Belgium, Brazil, Bulgaria, Canada, Chile, Colombia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Luxembourg, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Russian Federation, Slovak Republic, Slovenia, South Africa, Spain, Sweden, Switzerland, Turkey, United Kingdom, and the United States. OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions: Ratification Status as of 20 Novemer 2012, *available at* http://www.oecd.org/daf/anti-bribery/antibriberyconventionratification.pdf.

[201] OECD Anti-Bribery Convention, *supra* note 190, at art. 1. The phraseology for who is a foreign public official differs among the Anti-Bribery Convention, FCPA, and Bribery Act. Under the Anti-Bribery Convention, a foreign public official is "any person holding a legislative, administrative or

one made intentionally in order to induce a foreign official to act or to refrain from acting in relation to the performance of his official duties.[202] Obtaining or retaining business occurs if a party obtains a government contract. An improper advantage exists where a party makes a payment to receive something it is not clearly entitled to, such as a permit.[203] An illegal payment may be made either to a foreign official or another person or entity affiliated with the official, such as a family member or business.[204] Likewise, liability for the bribing party exists for payments that it makes directly, as well as for payments made indirectly through intermediaries.[205]

For defense vendors, the provisions of the Anti-Bribery Convention, FCPA, and Bribery Act pose three pressing problems. First, these laws' punishment of indirect payments make defense vendors liable for illegal payments made by sales or marketing agents, consultants, and joint venture partners.[206] Second, the definition of an "improper purpose" is broad enough to encompass bribery for the award of offset credit. Because offset credit relieves a defense vendor of financial liability to a purchasing government,[207] the illegal award of such credit would create an improper advantage for a bribing party. Finally, a "foreign official" may include not only employees of traditional foreign government agencies, but also employees of a

---

judicial office of a foreign country, whether appointed or elected; any person exercising a public function for a foreign country, including for a public agency or public enterprise; and any official or agent of a public international organization." *Id*. at art. 1(4). The Bribery Act largely adheres to this definition, varying only by making reference to countries or territories outside the United Kingdom. Bribery Act, c.23, § 6(5), 2010 (U.K.). However, under the FCPA, a foreign official is "any officer or employee of a foreign government or any department, agency or instrumentality thereof, or of a public international organization, or any person acting in an official capacity for or on behalf of any such government or department, agency, or instrumentality, or for or on behalf of any such public international organization." 15 U.S.C. §§ 78dd-1(f)(1), -2(h)(2), -3(f)(2) (2012).

[202] OECD Anti-Bribery Convention, Nov. 21, 1997, 37 I.L.M. 1, preamble, art. 1. Under the FCPA, a party must act with corrupt intent. 15 U.S.C. §§ 78dd-1(a), -2(a), -3(a). Although the FCPA does not define corrupt intent, courts interpreting this element have stated an act is with corrupt intent if done willfully, voluntarily, intentionally, and with a bad purpose of accomplishing either an unlawful end or result, or a lawful end or result by some unlawful method or means. U.S. v. Liebo, 923 F.2d 1308, 1312 (8th Cir. 1991); U.S. v. Kay (Kay III), 513 F.3d 461, 464 (5th Cir. 2007). The Bribery Act and Anti-Bribery Convention do not require corrupt intent; this was done in order to forestall any defenses alleging cultural norms or expectations that make a questionable payment legitimate. Warin, *supra* note 198, at 16; *see also* Bribery Act, c.23, § 6, 2010 (U.K.); OECD Anti-Bribery Convention, Nov. 21, 1997, 37 I.L.M. 1, art. 1 (lack of reference to corrupt intent).

[203] OECD Related Documents, *supra* note 199, at 14.

[204] *Id*. For FCPA liability for payments made to entities owned or affiliated with government officials, *see* Robert W. Tarun, The Foreign Corrupt Practices Act Handbook 7 (2d ed. 2012). For Bribery Act liability, *see* Ministry of Justice, The Bribery Act of 2010—Guidance, 2011, at 12-13 (U.K.).

[205] OECD Anti-Bribery Convention, Nov. 21, 1997, 37 I.L.M. 1, art. 1; *see also* 15 U.S.C. §§ 78dd-1(a), -2(a), -3(a); Bribery Act, 2010, c.23, § 6 (U.K.) (liability for indirect payments through intermediaries).

[206] OECD Related Documents, *supra* note 199, at 14; Tarun, *supra* note 205, at 7; Ministry of Justice, *supra* note 205, at 12-13.

[207] Gen. Accounting Office, GAO/NSIAD-96-65, *supra* note 10, at 2.

state-owned or state-controlled entity.[208] Because European governments frequently grant offsets to state-owned defense contractors,[209] vendors must confirm the status of foreign companies with whom they contract.

B. Commercial Bribery

Several federal and international laws prohibit commercial bribery in international transactions.[210] The Bribery Act prohibits commercial bribery when a financial advantage induces or rewards private persons for improperly performing functions in the scope of their employment or business.[211] Additionally, the U.S. Department of Justice (DOJ) may prosecute commercial bribery under the Travel Act if a bribing party used interstate travel or commerce to distribute the proceeds of bribery, or under the Federal Wire Fraud Act if a bribing party used transmissions in interstate commerce to promote a fraudulent scheme.[212] Although such prosecutions are rare,[213] defense vendors cannot ignore the risk of prosecution if, for example, a vendor's agent pays a subcontractor to generate forged invoices to earn offset credit.[214]

C. Recordkeeping and Internal Control Violations

In addition to prohibiting a bribe itself, international law criminalizes the maintaining of books and records that conceal or mischaracterize bribe transactions. The FCPA has two rules applicable to issuers of securities[215] in the United States: a requirement to make and keep accurate, reasonably detailed books and records, and a requirement to maintain an adequate system of internal accounting controls.[216] Although other countries impose similar duties to maintain adequate accounting records,[217] the FCPA is notable for its increasing number of enforcement actions.[218]

---

[208] Liability under the FCPA for a bribe to an employee of a state-owned enterprise is currently being litigated; however, so far courts have denied defense motions to dismiss prosecutions based on bribes to state-owned entities, deciding that the definition of a foreign official is a question of fact. U.S. v. Aguilar, 783 F. Supp. 2d 1108, 1115, 1120 (C.D. Cal. 2011).

[209] Georgopoulos, *Revisiting, supra* note 53, at 36.

[210] Warin, *supra* note 198, at 43.

[211] Bribery Act, c.23, § 6, 2010 (U.K.).

[212] 18 U.S.C. § 1952 (2002); 18 U.S.C. § 1343 (2008).

[213] To date, only one federal prosecution has resulted in a reported case charging commercial bribery under the Travel Act and Federal Wire Fraud Act. *See* U.S. v. Welch, 327 F.3d 1081 (2003) (discussing commercial bribery of members of International Olympic Committee).

[214] Transparency Int'l, Defence Offsets, *supra* note 11, at 14.

[215] An issuer of securities is a publicly traded company which files an application with the Securities and Exchange Commission to register on a national securities exchange. 15 U.S.C. § 78l(b) (2012).

[216] 15 U.S.C. § 78m(b)(2) (1998).

[217] *See* Warin, *supra* note 198, at 35 (accounting the requirements of U.K. Companies Act 2006).

[218] U.S. Securities and Exchange Commission, *SEC Enforcement Actions: FCPA Cases*, http://www.sec.gov/spotlight/fcpa/fcpa-cases.shtml (last visited May 24, 2012) (listing of growing number of

An FCPA recordkeeping violation occurs if an issuer fails to make and keep books, records, and accounts in reasonable detail that accurately and fairly reflect the transactions and dispositions of the issuer's assets.[219] The recordkeeping rule essentially requires a company paying a bribe to record the transaction as a bribe,[220] and not conceal the payment as another type of transaction such as a consultant fee or marketing expense.[221] An FCPA internal control violation occurs if an issuer fails to devise and maintain a system of internal accounting controls sufficient to meet objectives such as recording transactions in a way that permits asset accountability.[222]

D. Failure of a Commercial Organization to Prevent Bribery

The Bribery Act created a new offense in 2011 when it made businesses liable for failing to prevent persons associated with them from committing bribery.[223] This prohibition has been compared to the FCPA's recordkeeping and internal control provisions, because both the U.K. and U.S. laws require companies to operate internal anti-corruption programs for compliance.[224] However, the Bribery Act's provisions are broader than the FCPA's due to broader jurisdictional and liability standards.

A commercial organization fails to prevent bribery if a person associated with it bribes another person intending to retain business, or obtain or retain an advantage, for the commercial organization.[225] An "associated person" is anyone who performs services for or on behalf of the commercial organization.[226] The Bribery Act states an employee, agent, or subsidiary meets the definition of associated person, but contractors, suppliers, and joint venture partners may also fall within the definition.[227] Additionally, the person offering the bribe does not have to be

---

FCPA enforcement actions by the SEC per year). In 2010, the U.S. Department of Justice (DOJ) and Securities and Exchange Commission (SEC) had over 70 enforcement actions under the FCPA, with over $1.4 billion in fines. TARUN, *supra* note 205, at xxvii; LOUGHMAN & SIBERY, *supra* note 47, at 5.

[219] 15 U.S.C. § 78m(b)(2)(A) (1998).

[220] TARUN, *supra* note 205, at 13.

[221] OECD Bribery in Public Procurement, *supra* note 73, at 39-40; *see* FEINSTEIN, *supra* note 74, at 83 (categorizing of BAE Systems' bribes to Saudi officials as a marketing expense); Leigh & Evans, *Al-Yamamah*, *supra* note 3 (categorizing of BAE Systems' bribes to Saudi officials as a marketing expense).

[222] 15 U.S.C. § 78m(b)(2)(B) (1998). The FCPA's full requirements are that an issuer provide reasonable assurances that: (1) transactions are executed in accordance with management authorization, (2) transactions are recorded as necessary to permit preparation of conforming financial statements and maintain accountability for assets, (3) access to assets is permitted only according to management authorization, and (4) recorded accountability for assets is compared with existing assets at reasonable intervals and appropriate action is taken on discrepancies. *Id*.

[223] Bribery Act, c.23, § 7, 2010 (U.K.).

[224] Warin, *supra* note 198, at 8.

[225] Bribery Act, c.23, § 7(1), 2010 (U.K.).

[226] *Id*. at § 8(1).

[227] *Id*. at § 8(3); Ministry of Justice, *supra* note 205, at 16 (U.K.). Guidance by the U.K. Ministry of

prosecuted in order for the commercial organization to be held liable, and the bribe itself may be offered or given to either a commercial or governmental entity.[228]

The broad jurisdiction of the failure to prevent bribery offense is remarkable. The FCPA's recordkeeping and internal control provisions apply only to issuers of U.S. securities. However, the Bribery Act's failure to prevent bribery offense applies to any incorporated body or partnership which carries on a business, or part of a business, in any part of the United Kingdom.[229] The U.K. Ministry of Justice has stated merely listing securities in the United Kingdom, or the existence of a U.K. subsidiary, does not automatically mean a company is carrying on business in the United Kingdom. Additionally, the SFO Director has stated that "carrying on business" means "economic engagement" with the United Kingdom, such as trading, raising finance, carrying out corporate functions, or dealing with numerous stakeholders.[230] However, because the United Kingdom is one of the seven largest defense markets in the world,[231] it is likely a major defense vendor would conduct enough business in the United Kingdom to trigger liability under the Bribery Act.

E. False Claims In Foreign Military Sales

The FCA makes it illegal to knowingly present, or cause to be presented, a false or fraudulent claim for payment or approval by the U.S. government.[232] In United States ex rel. Campbell, the District Court for the District of Maryland held that invoices processed through FMS may create FCA liability if fraudulent.[233] Specifically, the court held that FMS invoices submitted to DOD met the FCA

Justice (MOJ) states the degree of control a company has over an entity will be taken into account in prosecution decisions, and the fact a company benefits indirectly from a third party's bribe is unlikely, by itself, to prove the entity intended to benefit the company. Ministry of Justice, *supra* note 205, at 17. However, this assurance is cold comfort because the MOJ determines if an offense occurred by examining the intent of the bribe-giving party; the crime of failing to prevent bribery imposes strict liability for the company. Bribery Act, c.23, § 7(1) 2010 (U.K.); Ministry of Justice, *supra* note 205, at 17; Tarun, *supra* note 205, at 432.

[228] Bribery Act, c.23, §§ 1, 6, 7(3)(a), 2010 (U.K.).

[229] 15 U.S.C. § 78m(a); Bribery Act, c.23, § 7(5), 2010 (U.K.).

[230] Ministry of Justice, *supra* note 205, at 15-16; Organisation for Economic Co-operation and Development, Phase 3 Report on Implementing the OECD Anti-Bribery Convention in the United Kingdom 15 (2012) [hereinafter OECD Phase 3 Report]; Loughman & Sibery, *supra* note 47, at 30.

[231] *World Wide Military Expenditures – 2011*, http://www.globalsecurity.org/military/world/spending.htm (last visited Sep. 7 2012); *Military Ranking: The World's Biggest Defence Budgets*, The Economist (Mar. 9, 2011, 2:57 PM), http://www.economist.com/blogs/dailychart/2011/03/defence_budgets.

[232] 31 U.S.C. § 3729(a)(1) (2009).

[233] United States ex. rel. Campbell v. Lockheed Martin Corp., 282 F. Supp. 2d 1324, 1329. 1340 (M.D. Fla. 2003). In the only other reported case to consider the question, the reasoning and holding of *United States ex. rel Campbell* was confirmed in United States ex rel. Hayes v. CMC Elec., Inc., 297 F. Supp. 2d 734, 737-738 (D.N.J. 2003).

definition of a claim for payment.[234] Additionally, the court held that even though FMS items are resold to a foreign government, and the U.S. government is reimbursed for all FMS expenses, this does not allow a defense vendor to escape FCA liability.[235] A vendor's fraudulent claim establishes FCA liability, and a subsequent government-to-government sale does not excuse or eliminate such liability.[236] Therefore, a false invoice, record, or statement from a subcontractor material to the prime vendor's invoice could result in FCA liability.[237] The FCA requires no proof of specific intent to defraud, but only actual knowledge of information, an act in deliberate ignorance of the truth or falsity of information, or reckless disregard of the truth or falsity of information.[238]

V. TRACING CORRUPTION PATHWAYS IN OFFSET TRANSACTIONS

Offset corruption risks exist at several points in a transaction. In the formation stage, a bribe may skew an offset's valuation as an award criterion, generate an unnecessary offset requirement, or determine a sole source offset award.[239] In the performance stage, an offset may operate as a sham transaction to siphon funds or may prompt a bribe in exchange for fraudulent offset credit.[240] These corrupt practices succeed through the exploitation of an offset's award criteria, valuation mechanisms, and sole sourcing provisions, and by utilizing non-transparent procurement processes.

A. Formation of Offset Proposals

During the negotiation and award of a defense procurement, a party may bribe a foreign official in order to improperly award a defense procurement to a particular foreign vendor, or to improperly award an offset subcontract to a particular domestic contractor.[241] To make a corrupt award seem legitimate, a foreign official may manipulate an offset's valuation and sole sourcing rules.

To bribe a foreign official, a party will most frequently arrange for an electronic transfer of money from an intermediary into a corrupt official's bank account.[242] Alternately, a party may deliver its bribe through tangible assets such

---

[234] 31 U.S.C. § 3729(a)(1) (2009). *Campbell*, 282 F. Supp. 2d at 1329, 1340.

[235] *Campbell*, 282 F. Supp. 2d at 1342.

[236] *Id*.

[237] 31 U.S.C. §§ 3729(a)(1)(A), 3729(a)(1)(B) (2009).

[238] *See* 31 U.S.C. §§ 3729(b)(1) (2009) (FCA definition of knowledge).

[239] *See* Feinstein, *supra* note 74, at 177-178, 182 (displaying the offset valuation scheme in South African procurement); Transparency Int'l, Defence Offsets, *supra* note 11, at 18-19, 43 (discussing corruption in award of offsets).

[240] Feinstein, *supra* note 74, at 83-84; Transparency Int'l, Defence Offsets, *supra* note 11, at 17.

[241] *See* Transparency Int'l, Defence Offsets, *supra* note 11, at 18 (list of corruption risks in offsets).

[242] OECD Bribery in Public Procurement, *supra* note 73, at 47.

as cash, gifts, travel, and entertainment.[243] Bribers often use an intermediary to deliver a bribe, such as an agent, consultant, or an official's family member, in order to conceal their own identities.[244]

Some observers, including former Senator Russell Feingold, have argued that defense offsets in and of themselves are a bribe.[245] However, it is important to distinguish between an offset serving as a bribe, versus an offset as an object for a bribe. A bribe exists if a person offers an undue payment to a foreign official in order to obtain or retain business.[246] For example, in South Africa a foreign vendor awarded an offset contract to a company that later, allegedly, issued some free company shares to the South African defense minister.[247] In this instance, the company's stock gift to the defense minister was a bribe.[248] However, the offset itself was not a bribe; instead, it was the business the bribe sought to obtain. Anti-bribery laws do not outlaw the operation of legitimate business, and offsets, despite their nature as contractual incentives, deliver products and services that benefit the purchasing government.[249] Offsets do not offer a unique way to exchange undue payments in a bribe transaction; instead, they are unusual in how they exploit procurement mechanisms to unlawfully award a contract. In the contract formation process, procurement valuation and subcontracting are exploited to reward bribery.

In an improper valuation scheme, a government official improperly inflates an offset's valuation to award a defense procurement to a corrupt vendor as a payback for a bribe.[250] For this scheme to work, an offset must be an award criterion, and government officials must abuse their discretion in valuing offset proposals.[251]

---

[243] *See Id*. at 47 (showing forms that a bribe may take).

[244] *See Id*. at 38-40, 41-42 (displaying the use of intermediaries to offer bribes in government procurement).

[245] Charles M. Sennott, *US Sees Conflict of Interest over Arms Commerce*, Boston Globe, May 9, 1996, at 1. In addition, one economist has called the issuance of offsets "the equivalent of what we used to do when we bribed foreign officials. Leslie Wayne, quoting Robert E. Scott, *A Well-Kept Military Secret*, N.Y. Times, Feb. 16, 2003, § 3 at 1. Finally, other observers have equated offsets to "bribes and corporate welfare." Derrick Z. Jackson, *US Plays the Arms Sales Game*, Boston Globe, Feb. 21, 2003, at A19.

[246] OECD Anti-Bribery Convention, Nov. 21, 1997, 37 I.L.M. 1, art. 1; 15 U.S.C. §§ 78dd-1. -2, -3; Bribery Act, c.23, § 6, 2010 (U.K.).

[247] Feinstein, *supra* note 74, at 181.

[248] *Living with the U.S. Foreign Corrupt Practices Act (FCPA) in an Era of Enhanced Enforcement*, 22 SPG Int'l Law Practicum 3, 5 (2009) (gift of stock as a bribe under the FCPA). Such a transaction may also constitute a bribe under local bribery laws; *see* Daniel Y. Jun, *Bribery Among the Korean Elite: Putting an End to a Cultural Ritual and Restoring Honor*, 29 Vand. J. Transnat'l L. 1071, 1090 (1996) (state official's receipt of stock acted as a bribe under Korean bribery law); OECD Bribery in Public Procurement, *supra* note 73, at 47 (gift of stocks as a bribe).

[249] *See* sections II.A. and II.C of this article for a discussion of offset incentives, products and services.

[250] *See* Feinstein, *supra* note 74, at 177-178, 182 (offset valuation scheme in South African procurement).

[251] *See* Eriksson, *supra* note 33, at 30 (offsets used as an award criterion in E.U. Member States);

Offset valuation is prone to improper inflation because offset cost figures, even within legitimate deals, are complicated by several risk factors. First, valuation involves the use of proprietary source selection data, so valuation information cannot be disclosed to outside parties for public oversight.[252] Second, because offsets allocate direct offset work to domestic contractors which are not as efficient as their international competitors, offsets require vendors to add a cost premium to a defense acquisition.[253] This cost premium depends on production costs (e.g., an item's price and marketability in countertrade), as well as transaction costs (e.g., exchange rate, inflation, and default risks).[254] Third, offset valuation may be complicated by the unavailability of market data for the subject of an offset, or by a lack of reliable data on how successfully an offset recipient will fulfill its contract.[255] Fourth, valuing an offset may be speculative if it requires a defense vendor to develop new business for an offset recipient by investing money, skill, or technology into that firm. The offset may condition the offset's discharge on the investment's success, yet such an outcome is unknowable at the time of offset formation.[256] Fifth, and most crucially, offset valuation may be improperly inflated if purchasing governments do not value an offset on cost, but instead on complex formulas.[257] For example, to value technology transfer, offset parties may utilize the item's reproduction cost, replacement cost, projected production run, estimated income stream, or anticipated future profits.[258]

These multiple risk factors make valuing an offset highly speculative. For example, when the consortium producing the Eurofighter Typhoon bid on a Norwegian fighter jet procurement in 1999, several billion dollars separated the offset valuations calculated by the defense vendor (26.7 billion Norwegian krone, or $4.4 billion), Norwegian industry (16 billion Norwegian krone, or $2.6 billion), and the Norwegian defense ministry (4.5 billion Norwegian krone, or $740 million).[259] In this

---

Feinstein, *supra* note 74, at 177-178, 182 (manipulation of offset valuation in a South African procurement).

[252] For example, in U.S. procurements, proposed costs or prices constitute protected source selection information. FAR § 2.201 (2013). The U.S. government is prohibited from disclosing cost or pricing data to a purchasing government without the consent of the vendor. DFARS § 225.7304(c) (2012); DoD 5105.38-M, *supra* note 72, at C6.3.9.1.

[253] Markowski & Hall, *supra* note 58, at 49.

[254] Robert Howse, *Beyond the Countertrade Taboo: Why the WTO Should Take Another Look at Barter and Contertrade*, 60 U. Toronto L.J. 289, 310 (2010).

[255] Nobles & Lang, *supra* note 112, at 749 (discussing offset valuation as a weak point); Gen. Accounting Office, GAO/NSIAD-96-65, *supra* note 10, at 2 (showing a lack of market data); Markowski & Hall, *supra* note 58, at 47, 49 (showing a lack of market data and imperfect data on merits of a local contractor).

[256] *See* Dumas, *supra* note 17, at 23-24 (showing the risk of failure when defense vendors work as venture capital firms for offsetting companies).

[257] *See* Jang et al., *supra* note 100, at 93; UNCITRAL Legal Guide, *supra* note 100, at 71-72 (discussing the valuation of technology transfer based on estimated future royalties).

[258] Jang et al., *supra* note 100, at 93-94; UNCITRAL Legal Guide, *supra* note 100, at 71-72.

[259] Matthews, *supra* note 105, at 98; The Money Converter, *supra* note 3.

instance, the purchasing government acted as a brake on optimistic offset valuations. However, with a corrupt government, the offset valuations in the Norwegian example could be turned on their head, with a corrupt official overselling an offset's value in exchange for a bribe.

Unfortunately, such an allegation of corrupt offset manipulation was raised in the procurement of a training jet in South Africa.[260] In a three-way competition, a British bid allegedly received the lowest score on both technical and cost criteria, but when the South African Defense Ministry factored financing and a substantial offset proposal into the bid, they ranked the British proposal as the most advantageous.[261] When the South African Department of Trade and Industry (SADTI) conducted its own analysis of the British offset's valuation, SADTI disputed the offset valuation, stating the value was "grossly inflated" from $245 million to $1.6 billion.[262] Nevertheless, the British bid won the South African contract.[263] Anti-corruption advocates allege that bribery caused the South African offsets valuation to increase by a factor of six.[264]

Corrupt officials may also exploit offset subcontracting rules to reward a bribe. Specifically, a potential offset recipient may bribe a government official to direct the prime vendor to award an offset to the bribing party.[265] Such a bribe could occur in two parts of the procurement process: the creation of offset proposals where an official could create an offset to benefit a particular local company, and the award of offset subcontracts.[266]

In offset negotiations, a bribe to create an improper offset could be obscured among the hundreds of offset proposals that are typically reviewed for a final offset package.[267] Moreover, an improperly influenced offset proposal could enter into discussions through the input of third parties pitching a reverse piggyback offset to a vendor's offset agents.[268] By inserting an offset proposal through a third party, a corrupt government official could effectively mask his or her involvement in the deal.

---

[260] Feinstein, *supra* note 74, at 177, 182.

[261] *Id*. at 177-178.

[262] *Id*. at 178.

[263] *Id*. at 180.

[264] *Id*. at 179.

[265] See Loughman & Sibery, *supra* note 47, at 298.

[266] Transparency Int'l, Defence Offsets, *supra* note 11, at 17-18.

[267] *See* Gen. Accounting Office, GAO-04-954T, *supra* note 62, at 1 (offset negotiations required prior to contract award); Redlich & Miscavage, *supra* note 39, at 403 (providing over 100 offset opportunities identified in offset negotiations with Israel); Seguin, *supra* note 37, at 22 (citing 104 offset commitments in F-16 sale to Poland).

[268] Gen. Accounting Office, GAO/NSIAD-96-65, *supra* note 10, at 1 (showing offsets as a condition initiated by a purchaser); Marvel, *supra* note 101, at 36 (identifying "reverse piggyback offsets" initiated by third parties).

In the award phase, government officials could direct a defense vendor to award an offset to a particular subcontractor on dubious national security or industrial development grounds. For example, an Asian government that purchased an airplane through FMS in the 1990s specified that it would select the companies which would manufacture the airframe in accordance with an offset.[269] The country justified directed award by stating all four selected aerospace subcontractors needed to achieve a proportionate share of subcontracting work.[270] In defense procurement, such apportionments are often made in the interest of national security so more than one defense vendor remains capable of manufacturing a key weapon component.[271] However, if a directed award is tainted by corruption, the rationale may actually legitimize an improper offset award.[272]

B. Award of Offset Credit

In the performance phase of an offset, there are two ways for corruption to affect an offset transaction. First, an offset can be a sham transaction used to siphon funds to government officials.[273] Second, a vendor may offer a bribe to improperly receive offset credit to discharge an offset obligation.[274]

In sham transactions, an offset may be used to generate false claims against a purchasing government in order to siphon funds to corrupt government officials and commercial parties. A scheme for sham transactions may originate as early as the negotiation of an offset package; for example, corrupt officials and companies may agree to generate sham transactions to reimburse the vendor for its bribery costs.[275] Bribery typically occurs over many years, and corrupt officials collect bribes throughout the course of a business relationship.[276] Therefore, if a vendor can obtain a corrupt official's agreement, a vendor may choose to file false claims to shift the bribery burden onto the purchasing government. This is illustrated by

---

[269] U.S. Gen. Accounting Office, GAO/NSIAD-99-35, Defense Trade: U.S. Contractors Employ Diverse Activities to Meet Offset Obligations 5 (1998) [hereinafter Gen. Accounting Office, GAO/NSIAD-99-35].

[270] *Id.*

[271] In a U.S. procurement, the manufacturing of the F-35's jet engines was directed to be awarded to two U.S. manufacturers—General Electric and Pratt Whitney—on the grounds that it was required to maintain the defense industrial base, and that it was required to lower prices through competition. Penny Wise, Pound Foolish F-35 Alternate Engine Recommendation Should be Rejected by Congress…Again, Bartlett (February 14, 2012), http://bartlett.house.gov/news/documentprint.aspx?DocumentID=225080; Gen. Accounting Office, GAO-03-775, *supra* note 165, at 1.

[272] *See* Transparency Int'l, Defence Offsets, *supra* note 11, at 14 (cronyism and nepotism as incentives for bribery in award of offsets).

[273] *See* Leigh & Evans, *Al-Yamamah, supra* note 3; Pallister, *supra* note 3, at 9 (discussing reimbursement of bribes in Al Yamamah contracts); Feinstein, *supra* note 74, at 83-84.

[274] Transparency Int'l, Defence Offsets, *supra* note 11, at 14, 17.

[275] *See* Leigh & Evans, *Al-Yamamah, supra* note 3; Pallister, *supra* note 3, at 9.

[276] OECD Bribery in Public Procurement, *supra* note 73, at 45.

the alleged bribery that occurred between BAE and corrupt Saudi officials.[277] The initial bribes in BAE's Saudi contracts are estimated to be between £300 and £600 million ($460 million and $921 million), but the total amount of bribery over the course of the twenty-year Saudi contracts are estimated to be over £6 billion ($9.7 billion).[278] Throughout the duration of its Saudi contracts, BAE allegedly bribed Saudi officials through false commissions and hospitality payments,[279] which it would falsely record as "marketing services" or "accommodation, services and support for overseas visitors."[280] In addition, BAE allegedly hid bribes in inflated bills from Saudi subcontractors.[281] To obtain reimbursement for its bribes, BAE allegedly charged its mischaracterized expenses to the U.K. Ministry of Defense, which would then seek reimbursement from the Saudi government, as is done in an FMS government-to-government contract.[282]

A second way for offsets to serve as a basis for corruption is for a defense vendor to offer a bribe in order to discharge an offset obligation.[283] Such a corrupt payment may be offered as a bribe to a commercial entity to obtain fraudulent offset documentation,[284] to a government official to grant unearned offset credits,[285] or in response to a government official's extortion.[286]

---

[277] BAE Systems has not admitted to or been found guilty of bribery in the Al Yamamah scandal. In February 2010, it entered into an agreement with the SFO admitting to bribery in Tanzania, but not in Saudi Arabia. OECD Phase 3 Report, *supra* note 231, at 15. In March 2010, BAE Systems pled guilty in the U.S. to making false statements, but did not plead guilty to bribery. Press Release 10-209, Dep't of Justice, *BAE Systems PLC Pleads Guilty and Ordered to Pay $400 Million Criminal Fine*, (Mar. 1, 2010), *available at* http://www.justice.gov/opa/pr/2010/March/10-crm-209.html. Such a result occurred, in no small part, because in December 2006 Saudi officials threatened to cease co-operation with the U.K. on intelligence and security issues if the U.K. continued to investigate allegations that BAE Systems had bribed Saudi officials to the Al Yamamah contract. In response to this threat, the SFO terminated its investigation in the Al Yamamah case. Despite calls by the OECD, among others, for the U.K. to re-open the Al Yamamah investigation, the SFO has declined to do so. OECD Phase 3 Report, *supra* note 231, at 15.

[278] Feinstein, *supra* note 74, at 76; Leigh & Evans, *Al-Yamamah, supra* note 3; *see* The Money Converter, *supra* note 3, for conversion from U.K. pounds to U.S. dollars.

[279] Feinstein, *supra* note 74, at 75, 79-80.

[280] *Id*. at 83; Leigh & Evans, *Al-Yamamah, supra* note 3.

[281] Leigh & Evans, *Al-Yamamah, supra* note 3; *see* The Money Converter, *supra* note 3, for conversion from U.K. pounds to U.S. dollars.

[282] Feinstein, *supra* note 74, at 83-84; Pallister, *supra* note 3, at 9; see DISAM, *supra* note 170, at 9-20 (showing that the U.S. government is the "banker" for offset transactions in FMS).

[283] Transparency Int'l, Defence Offsets, *supra* note 11, at 14, 17.

[284] *Id*. at 17.

[285] *Id*. at 14.

[286] OECD Bribery in Public Procurement, *supra* note 73, at 46; *Lockheed's Commission Payments to Obtain Foreign Sales: Report to the Chairman, Subcomm. On Banking, Housing and Urban Affairs*, 95th Cong. 7 (1977) (statement of Robert F. Keller, Acting Comptroller General) (stating that bribes paid overseas were usually made as a grease payment, a payment to secure competitive advantage, or a payment in response to extortion).

A commercial bribe for false offset documentation could occur either as a bribe to obtain false invoices, or a bribe to obtain fraudulently banked offset credits.[287] Alternately, a vendor may bribe a government official to receive unearned offset credit,[288] achieved through manipulating offset valuation formulas or giving credit for non-offset work. For example, in South Africa, a Swedish company received an indirect offset to upgrade a spa in Port Elizabeth, and to market travel to this spa to Swedish tourists.[289] The cost of the vendor's investment was $3 million, but the Swedish vendor allegedly claimed $218 million in offset credits because the offset allowed it to receive $3,830 in credit for each Swedish tourist traveling anywhere in South Africa, not just Port Elizabeth.[290] During the offset performance period, South Africa hosted the World Cup, so the Swedish vendor potentially received credit for every Swedish tourist in attendance, many of whom likely never visited the offset's spa.[291]

Finally, government officials may extort a bribe by manipulating offset valuation tools to create leverage. Over the last fifteen years, many countries have required vendors to deliver offsets valued at over one hundred percent of the original contract's purchase price.[292] Such valuations are created with the help of offset multipliers.[293] If a multiplier is used in a vendor's favor, it lessens the offset's cost burden.[294] However, a denial of credit for an offset with multipliers could also create pressure for a bribe. This is especially true if an offset has criteria which are difficult to satisfy, or if there are no alternate businesses with which to satisfy an offset.[295] If an offset agreement has penalty clauses,[296] a corrupt official may also leverage them for bribes. Although some countries allow vendors to accumulate and trade banked offset credits,[297] this practice does nothing to check offset officials' discretion in valuing and granting offset credits, and does not bring transparency to

---

[287] *See* Transparency Int'l, Defence Offsets, *supra* note 11, at 17 (bribes for false invoices); Verma, *supra* note 117, at 1 (identifying concern over receipt of unearned banked offset credits).

[288] *See* Verma, *supra* note 117, at 1.

[289] Feinstein, *supra* note 74, at 180.

[290] *Id.*

[291] *Id.*

[292] Eriksson, *supra* note 33, at 30; *see also* Dep't Of Commerce, Twelfth Study, *supra* note 33, at Appendix F (showing offsets as part of procurement decision).

[293] Gen. Accounting Office, GAO-04-954T, *supra* note 62, at 1.

[294] U.S. Gen. Accounting Office, GAO-01-278T, Defense Trade: Observations on Issues Concerning Offsets 1-2 (2000) [hereinafter Gen. Accounting Office, GAO-01-278T].

[295] *See* Gen. Accounting Office, GAO/NSIAD-96-65, *supra* note 10, at 4 (discussing the difficulty to satisfy United Arab Emirates' offsets due to their crediting only an offset's profit).

[296] Dep't of Commerce, Sixteenth Study, *supra* note 10, at 3. Penalty clauses may, for example, increase the amount of a required offset obligation, reduce the value of a signed export sales contract, or require liquidated damages. *Id*. Half of the offset agreements signed by U.S. companies in 2010 have penalty clauses. *Id.*

[297] Gen. Accounting Office, GAO-01-278T, *supra* note 295, at 3.

offset transactions.[298] Governments must significantly reform their national offset rules to prevent corrupt exploitation of offset mechanisms.

VI. REDUCING THE RISK OF DEFENSE OFFSET CORRUPTION

To deter and detect corruption throughout an offset's lifecycle, governments and defense vendors must undertake comprehensive reform measures. Specifically, the OECD should create an international convention defining basic standards for offset transparency, valuation, and competition. Additionally, defense vendors should heighten due diligence verification standards and increase the use of electronic audits.

A. Proposed OECD Convention on Offsets

To combat corruption and improve offset practice in general, the international community should establish minimum standards for offset regulation and management. Although past international efforts to regulate offsets have failed,[299] a current discussion of offset best practices is likely to bear fruit because in May 2011, the E.U.'s Code of Conduct on Offsets established a baseline of consensus among most OECD member states about offset management.[300] Specifically, the Code of Conduct requires member states to publish more information about their offset policies, practices, and existing offset commitments, and to clarify their offset requirements in contract solicitations and subcontract awards.[301] Using the Code of Conduct as a foundation, the OECD should create higher standards for international offset practice in the areas of transparency, offset valuation, and award of offset contracts.

1. Transparency Proposals

The Code of Conduct's transparency rules create a baseline for the OECD to initiate discussions for improved offset transparency. The Code of Conduct requires Member States to provide the European Defence Agency with information on their national offset practices and underpinning policies, and to disclose all offset commitments in effect since the Code of Conduct's implementation.[302] In addition, the Code of Conduct requires contract solicitations to clearly stipulate offset

---

[298] *See* Transparency Int'l, Defence Offsets, *supra* note 11, at 16 (showing discretion and secrecy in offsets).

[299] *See* Bialos, *supra* note 30, at 96 (illustrating past unsuccessful OECD offset discussions).

[300] *See* Code of Conduct on Offsets, *supra* note 153, at 1 (discussing the Code of Conduct promulgation in 2011). The OECD currently has 34 members, 20 of which are E.U. Member States. *See* http://www.oecd.org/about/membersandpartners (OECD members); http://europa.eu/about-eu/countries/index_en.htm (EU Member States).

[301] Code of Conduct on Offsets, *supra* note 153, at 3-4.

[302] *Id*. at 3.

requirements and to make clear if offset is an award factor.[303] Although these rules provide some clarity to offset award and offset practices in general, the international community should do more to give contractors and third parties better information on the offset decision-making process.[304] Specifically, the OECD should promote transparency during the offset's solicitation, offer, and award phases.

During solicitation, purchasing governments should clearly state their offset requirements and make a declaration of whether offsets are an award criterion, as recommended by the Code of Conduct.[305] In addition, purchasing governments should publish the valuation formulas they intend to use to assess offset proposals. Although it is inherently difficult to make projections on a proposal's future production, sales, or profits, as is frequently done in technology transfer offsets,[306] the disclosure of valuation formulas would show whether a purchasing government is using reliable and relevant criteria to calculate an offset's value, or is using a method at risk for overstating projected benefits.[307] Formula publication promotes the use of defensible formulas for economic projections, and deters government officials from abusing their discretion.[308]

In the offer phase, offerors should separately account for offset transaction costs so purchasing governments may more accurately assess the benefits of purchasing an offset.[309] Accounting for such costs would depend on whether an offset is direct or indirect. Indirect offset costs are unrelated to the costs of the defense item and could easily be broken out.[310] However, direct offsets for items such as aircraft components are integral to the weapon system's price.[311] Therefore, to break out a direct offset's true cost, a vendor must disclose how much the component costs when manufactured both in the vendor's country and in the purchasing country. Such information constitutes proprietary data that a vendor

---

[303] *Id*. at 4.

[304] Transparency Int'l, Due Diligence and Corruption Risk in Defence Industry Offset Programmes 31 (2012) [hereinafter Transparency Int'l, Due Diligence]; *see also* OECD Bribery in Public Procurement, *supra* note 73, at 67 (showing the need for increased transparency to increase detection risk for corrupt activity).

[305] Code of Conduct on Offsets, *supra* note 153, at 3-4.

[306] *See* UNCITRAL Legal Guide, *supra* note 100, at 72-73 (discussing the valuation of technology transfer based on a lump-sum payment, or a payment of royalties that is linked to projections of future production, sales or profits).

[307] Transparency Int'l, Due Diligence, *supra* note 305, at 36.

[308] *See* OECD Bribery in Public Procurement, *supra* note 73, at 67 (illustrating that the lack of transparency in national security procurements fails to provide a deterrent to corrupt activity).

[309] Transparency Int'l, Due Diligence, *supra* note 305, at 35.

[310] *See* Dep't of Commerce, Sixteenth Study, *supra* note 10, at 5, 27 (defining indirect offset); Dumas, *supra* note 17, at 21 (showing offsets as providing discounts for offset items, or merely constituting secondary purchases).

[311] *See* Dep't of Commerce, Sixteenth Study, *supra* note 10, at 5, 27 (defining direct and indirect offset).

may be reluctant to disclose.[312] Additionally, current FMS rules prohibit the U.S. Government from disclosing contractor proprietary data to a purchasing government without vendor authorization.[313] The U.S. government justifies this FMS policy by citing a perception that foreign governments do not want to highlight offset costs, and U.S. defense contractors do not want offset costs disclosed because they are concerned that a foreign government may refuse to pay for them.[314] However, in its own procurements, the U.S. Government increasingly requires offerors to provide uncertified cost and pricing data whenever the head of a procurement activity deems it necessary.[315] Moreover, it seems disingenuous to assert that a foreign government will be more willing to pay for an offset if it is kept ignorant of its cost. Instead of retroactively policing corruption through criminal statutes such as the FCPA, Bribery Act, and Anti-Bribery Convention, governments should promote offset cost transparency to prevent corruption from occurring in the first place.

Once an award occurs, purchasing governments should publicly disclose data on each offset recipient to maximize public awareness of how the government is spending the public's money. Disclosed information should include the names and addresses of local offset subcontractors, places of execution or performance, nature of the offset products or services to be supplied, and performance time limits.[316] Although the United States does not require publication of the names of defense subcontractors, the European Union does require it as a transparency measure.[317] A robust publication rule assists the general public in a purchasing country to judge for themselves whether a particular offset is corrupt, a politically-driven subsidy, or meritorious.[318]

---

[312] Proposed costs or prices constitute protected source selection information. FAR § 2.201 (2012).

[313] DFARS § 225.7304(c) (2012); DoD 5105.38-M, *supra* note 72, at C6.3.9.1 (providing that the U.S. Government is prohibited from disclosing cost or pricing data to a purchasing government without the consent of the vendor).

[314] Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, *Offsets of Foreign Military Sales: FMS Offsets and Other Issues Affecting FMS Procurements Frequently Asked Questions (FAQs)*, http://www.acq.osd.mil/dpap/cpic/ic/offsets_of_foreign_military_sales.html#q4 (last visited Jul. 30, 2012); DoD 5105.38-M, *supra* note 72, at C6.3.9.1.

[315] 10 U.S.C. § 2306a(c) (2012); 41 U.S.C. § 254b(c) (2012).

[316] *See* 2009 Directive, *supra* note 74, at art. 52, Annex V (discussing the requirement for tenderers who are not contracting authorities to publish subcontract awards above a certain threshold).

[317] In U.S. federal contract award notifications, only the name of the prime contractor is required for publication. FAR § 5.207(a) (2012). However, this is not the case in E.U. defense procurements. 2009 Directive, *supra* note 74, at art. 52, Annex V.

[318] For criticism of offset recipients, *see* Taylor, *supra* note 29, at 38 (discussing offsets as subsidies for politically favored parties); Markowski & Hall, *supra* note 58, at 49 (discussing offsets as subsidies to support inefficient local subcontractors); Markusen, *supra* note 50, at 74 (discussing offsets redistributing production to second-best producers in foreign countries); Transparency Int'l, Defence Offsets, *supra* note 11, at 14 (discussing corruption in offsets).

2. Valuation Proposals

The OECD should promote rules that reign in valuation practices that distort an offset proposal's true value. Although the Code of Conduct requires E.U. member states to value offsets at a less significant weight than other award criteria in order to assure a procurement is based on best value, and to value offset proposals at no more than the total value of the defense sales contract,[319] these measures are insufficient to prevent the manipulation of offset values for corrupt purposes. In addition to adopting the Code of Conduct's restrictions, the OECD should also restrict the range of discretion government officials have in choosing offset multipliers.

The problems of offset valuation andoffset over-valuation corruption have prompted both the European Union and Transparency International to recommend that offsets either receive less weight in award decisions than other economic factors, or no weight at all.[320] However, from an anti-corruption perspective, an offset's weight as an award criterion is not the most effective area upon which to focus offset reform efforts. First, because offsets currently constitute such a large percentage of the value of foreign defense sales contract (e.g., their value in U.S. vendor contracts is 63.5 percent),[321] it is not practical to require purchasing governments to give no consideration, or little consideration, to offsets. Offsets are simply too valuable to ignore. Second, Poland's F-16 purchase showed that an award criterion with the small comparative weight of fifteen percent, when compared to forty-five percent for price and forty percent for tactical criteria, can still be decisive when other criteria are evenly matched among bidders.[322] Third, the weight assigned to offsets as an award criterion is not particularly susceptible to corrupt exploitation, because the weight assigned to an award criterion affects all offerors equally. Instead of focusing on offset weight, anti-corruption advocates should focus on valuation tools such as offset multipliers, minimum value requirements, and valuation formulas that can manipulate an individual offeror's ratings.

Offset multipliers and minimum value requirements work together in a self-reinforcing spiral that distorts offset valuation. Purchasing governments often require minimum offset valuations which equal or exceed the value of the underlying defense sale, and they express their offset demands as a percentage of the value of the defense sales contract's price, not as an independent dollar figure.[323] However, offsets are not a "free lunch." Defense vendors must cover offset costs by increasing the total price of a defense sales contract, or by using multipliers to meet minimum

[319] Code of Conduct on Offsets, *supra* note 153, at 4.

[320] *Id*. at 4; Transparency Int'l, Due Diligence, *supra* note 33 (2012).

[321] Dep't of Commerce, Sixteenth Study, *supra* note 10, at 3.

[322] *See* Seguin, *supra* note 37, at 11, 16, 30-31 (providing the weight of offset, price and technical criteria in Poland's procurement for fighter aircraft in 2002, and the final calculus that resulted in the F-16 winning the Polish procurement).

[323] Gen. Accounting Office, GAO-04-954T, *supra* note 62, at 1; Gen. Accounting Office, GAO/NSIAD-96-65, *supra* note 10, at 2; Eriksson, *supra* note 33, at 30.

offset requirements.[324] Multipliers are the only real means to reduce an excessive minimum offset demand, because an increase in the price of a defense sales contract only further increases that contract's offset requirement. Obtaining a high multiplier, then, becomes crucial for a vendor's success. Although all offerors must meet the same minimum offset requirement,[325] if offsets are an award criterion,[326] and if a procurement authority has discretion on what multiplier to assign to a specific offset proposal,[327] then a corrupt vendor has incentive to offer a bribe in exchange for a high multiplier that increases the value of its bid. When a government official is able to multiply an offset proposal by a factor ranging anywhere between ten to thirty times its actual value,[328] the temptation to bribe for a high multiplier is apparent.

Advocates for multipliers tout them as reducing the dollar burden of offset obligations, and as encouraging specific types of offset activity the purchasing government wishes to promote.[329] However, this argument does not acknowledge that in the current highly competitive defense market, it is not necessary to use multipliers to encourage offset activity. In a Kuwaiti procurement, for example, the government only required offsets worth thirty percent of the contract's value, yet the winning bid's offset package was worth 333 percent of the underlying contract's value.[330] To stay competitive in such a procurement, an offeror has no choice but to meet a purchasing government's offset demands.

To remedy the corruption risk posed by multipliers and offset value requirements, the OECD should narrow the discretionary range government officials have in calculating multiplier values, and cap total offset valuation at one hundred percent of the defense contract's value. Government officials must have discretion in calculating offset value to determine best value, but it seems excessive, to the point of inviting abuse, to give government officials the ability to multiply offset value by a factor between ten and thirty.[331] A narrower multiplier range, such as assigning a factor between zero and two, would be more temperate. Putting a maximum limit on offset valuations would require more selective multiplier use, and thereby put a needed check on offset officials' discretion.[332]

---

[324] Gen. Accounting Office, GAO-04-954T, *supra* note 62, at 1; Brauer & Dunne, *supra* note 13, at 2.

[325] *See* Gen. Accounting Office, GAO-04-954T, *supra* note 62, at 1.

[326] *See* Eriksson, *supra* note 33, at 30 (offsets used as an award criterion in E.U. Member States).

[327] *See* Dep't Of Commerce, Twelfth Study, *supra* note 33, at Appendix F (showing multipliers in use in countries such as Poland and the Netherlands).

[328] *Id*. (showing multipliers in use in the Netherlands).

[329] Gen. Accounting Office, GAO-04-954T, *supra* note 62, at 1; Georgopoulos, *Revisiting, supra* note 53, at 36.

[330] Redlich & Miscavage, *supra* note 39, at 387.

[331] *See* Dep't Of Commerce, Twelfth Study, *supra* note 33, at Appendix F (providing offset multipliers of up to 30 in the Netherlands).

[332] *See* U.S. Gen. Accounting Office, GAO/NSIAD-93-184, Military Sales to Israel and Egypt: DOD Needs Stronger Controls Over U.S.-Financed Procurements 33-34 (1993) (discussing the problem of offset value inflation).

3. Competition Proposals

Finally, the OECD should set standards that more strictly define when a purchasing government may direct an offset to a local contractor. The Code of Conduct states that E.U. member states will allow foreign suppliers to select the most cost effective business opportunities within a purchasing country for offset fulfillment, which enables fair and open competition where appropriate.[333] However, this formulation leaves an open question as to when it is appropriate to enable fair and open competition. The Code of Conduct is unclear on whether national security grounds may allow a member state to direct an offset award to a local contractor.[334] To clarify this exception to competition, the OECD should specify that directing awards on national security grounds should be done only in reference to components directly related to a defense item, and that indirect offsets should be awarded through full and open competition.

Because directed awards may serve as the reward for a bribe, it would be ideal to place strict conditions on all mandated awards, regardless of whether they are directly or indirectly related to an offset. However, restricting mandated awards in the sphere of direct offsets is not feasible for national security and political reasons. Specifically, purchasing governments require direct offsets, such as technology transfer for key weapons components,[335] in order to reduce the threat posed by disruptions to security of supply, and to retain some technological control over a defense item.[336] Additionally, purchasing governments mandate that direct offsets be awarded to specific companies in order to keep a local defense contractor solvent, or to spread offset work equally among defense contractors.[337] Although offset critics allege the national security rationale has been abused to exempt defense procurements (particularly offsets) from regular procurement rules, in reality it is difficult to scrutinize whether defense procurement sourcing decisions are truly

[333] Code of Conduct on Offsets, *supra* note 153, at 4. The Code of Conduct qualifies appropriateness by referring to efficiency, practicality, and economic or technical appropriateness. *Id*.

[334] National security grounds are not specifically referred to in the Code of Conduct, but they are implicit given that Article 296 of the Treaty Establishing the European Community allows member states to exempt military equipment from Community regulation. *Id*.; Consolidated Version of the Treaty Establishing the European Community art. 296, Dec. 29, 2006, C 321 O.J. 175.

[335] *See* Dep't of Commerce, Sixteenth Study, *supra* note 10, at 27 (depicting a pie chart on direct and indirect offsets).

[336] Green Paper, *supra* note 59, at 4-5 (discussing how offset requirements address security of supply and technological superiority concerns); Markowski & Hall, *supra* note 58, at 45-46 (discussing how offsets use local content requirements to source a portion of the contract value in the buyer's territory); Markusen, *supra* note 50, at 68 (discussing how transfer of technology is typical in offset packages).

[337] *See* Bialos, *supra* note 30, at 51 (Poland and Romania directing offset work to state-owned or controlled entities in order to keep them solvent); Gen. Accounting Office, GAO/NSIAD-99-35, *supra* note 270, at 5 (1998) (addressing how Asian government directed subcontract work to specific companies in order to spread offset work among multiple contractors in the same industry).

in the interest of national security.[338] Such decisions are inherent to a nation's sovereignty, and are political questions not subject to judicial review.[339] Therefore, regulating mandated awards for direct offsets is a non-starter. Instead, the OECD should form an international consensus for the proposition that national security concerns justify directing offset awards to companies producing a defense item and its components, but that mandated awards for indirect offsets are permissible only if otherwise allowable under a country's procurement rules.

Because indirect offsets are unrelated to a defense article or service, it may seem obvious that they are procured for economic reasons having no relation to national security interests or policies. [340] However, this is not an obvious conclusion in international defense trade. Defense products increasingly incorporate components designed for civilian use, such as aerospace software, into defense systems.[341] As a result, an indirect offset performed today could potentially benefit future business in a purchasing country's defense sector. Because of this cross-pollenation between certain civilian industries and the defense sector, some E.U. member states count offsets related to civilian sectors such as aerospace as direct offsets.[342] However, the OECD should prohibit such a loose definition of a direct offset. What should matter in characterizing an offset as direct or indirect is the intent of the offset when it is entered into. Potential uses that may not come to fruition are too speculative to form a basis for offset characterization, especially if such a characterization exempts an offset from competition.

B. Vendor Compliance Initiatives

To comply with anti-corruption statutes, defense vendors must institute compliance programs that prevent and detect criminal conduct.[343] Although anti-

---

[338] Heuninckx, *Procurement Directive, supra* note 60, at 2 (providing examples of E.U. Member States abusing Article 346 of the Treaty on the Functioning of the European Union to exempt their defense procurements from regular E.U. procurement rules); Eriksson, *supra* note 35, at 5 (showing a general difficulty in justifying any offset on national security grounds); Edwards, *supra* note 59, at 3 (showing difficulty of defining national security interests).

[339] Aris Georgopoulos, *The Commission's Interpretive Communication on the Application of Article 296 EC in the Field of Defence Procurement*, 16 Pub. Procurement L. Rev. 3, NA43, NA45 (2007); Nicolas Pourbaix, *The Future Scope of Application of Article 346 TFEU*, 20 Pub. Procurement L. Rev. 1, 1, at 7 (2011); *see also* ManTech Telecomms. & Info. Sys. Corp. v. United States, 49 Fed. Cl. 57, 75 n.27 (Fed. Cl. 2001) (stating that judicial deference is at its apogee in matters pertaining to the military and national defense, including matters pertaining to military requirements in defense procurements).

[340] Dep't of Commerce, Sixteenth Study, *supra* note 10, at 5, 27 (defining indirect offset); Taylor, *supra* note 29, at 40 (discussing justifications for indirect offsets).

[341] Georgopoulos, *Revisiting, supra* note 53, at 33.

[342] *See* Eriksson, *supra* note 33, at 16 (showing the variations in taxonomy among E.U. Member States regarding the definition of a direct offset).

[343] U.S. Sentencing Guidelines Manual § 8B2.1(a) (2011); Ministry of Justice, *supra* note 205, at 31; OECD Related Documents, *supra* note 199, at 31.

corruption statutes recognize that compliance program measures must be reasonable and in proportion to the corruption risk posed by the business relationship and transaction at issue,[344] this qualification is not helpful for defense vendors engaging in offsets. Specifically, offset corruption risks are among the highest in the defense sector[345] because offsets meet the criteria for nearly every corruption risk factor.[346] As a result, compliance measures for defense offset programs must necessarily meet a high standard. But if compliance programs are operated well, they may shield defense vendors from liability for an agent's criminal conduct. For example, when a former Morgan Stanley managing director in China pled guilty in 2012 to violating the FCPA by conspiring to evade the company's internal accounting controls,[347] DOJ declined to prosecute Morgan Stanley because it maintained a system of internal controls that included an internal policy prohibiting bribery; regular training on this policy; extensive due diligence on all new business partners; regular monitoring of transactions; and random audits of particular employees, transactions, and business units.[348] Due diligence and random audits are key components to compliance programs and to avoiding anti-corruption liability. Although due diligence and random audits are not low cost processes, defense vendors must improve their current level of compliance practice by heightening due diligence verification standards, and by executing electronic audits of offset partner documents.

1. Due Diligence Proposals

In a high risk transaction such as defense offsets, vendor due diligence should include investigations of proposed business partners' financial and business backgrounds, independent verifications of information provided by such potential partners, and periodic monitoring of business partners once a business relationship

[344] U.S. Sentencing Guidelines, Manual §§ 8B2.1(b)-(c) (2011); Ministry of Justice, *supra* note 205, at 27; OECD Related Documents, *supra* note 199, at 30.

[345] *See* Brian Loughman & Sibery, *supra* note 47, at 297-98 (asserting that offsets are singled out as one of the riskiest business practices for bribery and corruption in the aerospace and defense sector).

[346] The criteria for high corruption risk include conducting business in regions with a perceived high level of corruption such as Central Europe and the Middle East, conducting business in an industry that is high-risk for corruption due to its high transactional value and high level of interaction with government officials, and conducting business with intermediaries who must deal with politically exposed persons and prominent public officials. *See* Ministry of Justice, *supra* note 205, at 27 (listing the most common risk factors for corruption); Transparency Int'l, Corruption Perceptions Index, *supra* note 48, at 6-9 (listing the countries and geographical regions with high perceptions of corruption); Loughman & Sibery, *supra* note 47, at 296 (discussing the risks of corruption in the defense sector); Redlich & Miscavage, *supra* note 39, at 398 (discussing the extensive use of intermediaries who interact with government officials to form offset proposals).

[347] Press Release 12-534, Dep't of Justice, *Former Morgan Stanley Managing Director Pleads Guilty for Role in Evading Internal Controls Required by FCPA*, (April 25, 2012), *available at* http://www.justice.gov/opa/pr/2012/April/12-crm-534.html (discussing how the former Morgan Stanley director admitted to transferring a multi-million dollar ownership interest in a Shanghai real estate venture to a Chinese public official).

[348] *Id*.

is established.[349] However, there is evidence that such practices are uncommon. A recent study by Ernst & Young found that only forty-four percent of the sampled international companies performed due diligence background checks on third parties, and when such due diligence was performed, companies mostly relied on information from potential partners without verification.[350] These practices exist despite the fact that thirty-nine percent of international respondents said that bribery or corrupt practices occurred frequently in their countries, and that fifteen percent of international respondents were prepared to make cash payments to win or retain business.[351] On an equally pessimistic note, a separate study by Transparency International confirmed that while most defense companies conduct initial due diligence inquiries such as background checks and questionnaires, these investigations usually do not verify information from potential business partners due to the difficulty and expense of such efforts.[352] These practices are especially surprising when considering the substantial criminal liability for a corruption offense. For example, BAE paid the U.S. DOJ a $400 million criminal fine for allegations arising from its bribery scandal with the Saudi government.[353] Heightened due diligence is expensive, but not in comparison to such exorbitant criminal fines.

To conduct due diligence that effectively screens potential business partners for corruption risks, defense vendors must institute a thorough, multi-step vetting procedure. First, vendors should gain a general understanding of a potential business partner by conducting a public database background investigation into the party's executives, subsidiaries, and third-party intermediaries.[354] In addition, defense vendors should review documents provided by the party such as its anti-corruption policies, procedures, and training activities; business statements regarding its services and billing procedures; and questionnaire responses about areas of concern.[355]

Next, vendors should conduct face-to-face interviews with key executives, business references, and government officials to verify information provided by third-party and public databases.[356] Conducting such interviews in-country, preferably on a one-on-one basis, is critical to obtaining candid, reliable verification. Interviews

---

[349] Ministry of Justice, *supra* note 205, at 28; Loughman & Sibery, *supra* note 47, at 166, 170-171.

[350] Ernst & Young, *supra* note 44, at 2; Transparency Int'l, Due Diligence, *supra* note 305, at 4-5.

[351] Ernst & Young, *supra* note 44, at 2, 4.

[352] Transparency Int'l, Due Diligence, *supra* note 305, at 14, 18.

[353] Press Release 10-209, *supra* note 278. BAE Systems pled guilty to conspiring to defraud the U.S., making false statements about its FCPA compliance program, and violating the Arms Export Control Act and International Traffic in Arms Regulations. *Id*.

[354] Loughman & Sibery, *supra* note 47, at 71, 166; Ministry of Justice, *supra* note 205, at 28.

[355] Loughman & Sibery, *supra* note 47, at 71, 166; Ministry of Justice, *supra* note 205, at 28.

[356] Transparency Int'l, Due Diligence, *supra* note 305, at 14; Loughman & Sibery, *supra* note 47, at 167; Ministry of Justice, *supra* note 205, at 28.

should also include personnel who actually process business transactions, such as the finance manager, controller, and operations manager.[357]

After conducting interviews, vendors should follow up on red flags discovered in the potential partner's relationships or business practices. If these red flags are resolvable, defense vendors should seek to mitigate the risks posed by the red flags by instituting remedial measures. For example, they should require the third party certify its compliance with the vendor's compliance program, incorporate warranties into its offset contract, and obtain independent confirmation of offset completion from government officials or third-party sign-off panels before receiving payment for offset work.[358]

Finally, vendors should periodically conduct re-vetting procedures such as the ones listed above to confirm that a third-party is operating legally.[359] Confirmation from such periodic monitoring is especially necessary for offsets requiring several years to complete, and for offsets occurring in corruption-prone geographic areas.

2. Documentation and Auditing Proposals

To strike a balance between maintaining costs and maintaining compliance, defense vendors should increase offset documentation requirements and institute more automated record reviews to maintain accountability over offset transactions. Specifically, defense vendors should require business partners to provide more documentation as a prerequisite for payment, and should scan these documents with analytical software to search for irregular transactional patterns.[360] With these measures, vendors can increase the pool of data to search for red flags, and focus the efforts of traditional, on-site audits.

In Ernst & Young's report, data showed that companies currently underutilize documentation and auditing measures; specifically, only forty-five percent of international companies have contractual audit rights in place to monitor their business partners' anti-corruption compliance.[361] Even if agents and suppliers sign contracts giving their customers audit rights, it is questionable whether the rights are practically enforceable. Traditional audits consist of site visits, interviews, and

---

[357] Loughman & Sibery, *supra* note 47, at 170.

[358] Transparency Int'l, Due Diligence, *supra* note 305, at 16, 18-19; UNCITRAL Legal Guide, *supra* note 100, at 41.

[359] Transparency Int'l, Due Diligence, *supra* note 305, at 14; Ministry of Justice, *supra* note 205, at 31.

[360] Ernst & Young, *supra* note 44, at 10 (discussing the use of analytic software); Loughman & Sibery, *supra* note 47, at 124 (discussing the use of transaction testing); *see also* UNCITRAL Legal Guide, *supra* note 100, at 41-43 (discussing various methods to obtain documentation from business partners).

[361] Ernst & Young, *supra* note 44, at 10.

transaction testing, which are expensive to set up and execute.[362] Actually setting up an audit can take several months of negotiation, and several more in execution; as a result, an audit can be cost-prohibitive in terms of time and money.[363] In light of the global recession, companies are cutting back on labor-intrusive measures to remain competitive.[364] However, because document and accounting controls are key internal control features,[365] vendors must find a more cost effective means of maintaining accountability over their offset transactions.

In order to strike a new balance between maintaining compliance and reducing compliance costs, defense vendors should require business partners to provide multiple forms of documentation prior to payment, and should scan these documents with analytical software to detect red flags.[366] Such measures will replicate the thoroughness of traditional auditing site visits, yet leverage technology to reduce compliance costs.

Thorough documentation of offset transactions is critical to prove the offsets are legitimate, and to permit later data mining of these documents. For several decades, vendors have required offset partners to establish "evidence accounts" where they deposit copies of sales contracts, letters of credit, shipping documents, and other documentation to prove the existence of offset transactions.[367] Once documents were deposited in these accounts, defense vendors could retrieve them to confirm particular offset transactions.[368] For example, sales contracts and shipping documents could confirm whether a countertrade sale conformed with the quantity and price terms of an offset agreement, or resorted to dumping the offset product on world markets.[369] However, the usefulness of evidence accounts for electronic document scans has been limited because they have recorded mostly traditional sources of documentation.[370] To improve the utility of evidence accounts for data mining, offset contracts should also require offset partners to submit further

---

[362] OECD Related Documents, *supra* note 199, at 31; Ernst & Young, *supra* note 44, at 10.

[363] Sarah Johnson, *Don't Trust, Verify*, CFO Magazine, Feb. 1, 2012, http://www3.cfo.com/article/2012/2/ supply-chain_fcpa-third-parties-sec-compliance (discussing use of audit clauses in international industry); Romero, *supra* note 121 (discussing negotiation and expense required for audit of business partners).

[364] Ernst & Young, *supra* note 44, at 6.

[365] Loughman & Sibery, *supra* note 47, at 111.

[366] Ernst & Young, *supra* note 44, at 10 (discussing the use of analytic software); Loughman & Sibery, *supra* note 47, at 124 (discussing the use of transaction testing); *see also* UNCITRAL Legal Guide, *supra* note 100, at 41-43(providing various methods to obtain increased documentation from business partners).

[367] UNCITRAL Legal Guide, *supra* note 100, at 43.

[368] *Id*.

[369] *See* Brauer, *supra* note 67, at 55 (dumping offset products on the world market); Markowski & Hall, *supra* note 58, at 47 (discussing the default on offset obligations).

[370] *See* UNCITRAL Legal Guide, *supra* note 100, at 43 (discussing the use of evidence accounts to deposit sales contracts, letters of credit, shipping documents, etc.).

documentation such as offset-related correspondence with government officials and commercial agents, status reports on offset progress, and inventories of offset components. If evidence accounts contained this level of documentation, there would be sufficient information for a thorough document scan.

Once a vendor gathers its offset documentation, the vendor could scan these documents with a variety of automated tools to look for red flags. Analytical software tools come in three main forms: statistical analysis, text analysis, and data visualization. Statistical analysis runs numerical data through mathematical formulas in order to detect statistical anomalies.[371] Data analysis uses keyword searches to extract words by category, theme, or meaning in order to identify corrupt intent or improper payments.[372] Finally, data visualization integrates information from data and statistical analysis onto visualization dashboards to assist analysts in detecting anomalous patterns.[373] Such techniques are not perfect. Text analysis, for example, is unable to detect corrupt intent if local data privacy laws prohibit email searches without the prior consent of sending and receiving parties, or if analysts are unfamiliar with a foreign language's idioms and nuances.[374] However, these analytical tools allow vendors to scan more documents than personal review, and they allow vendors to expedite audits by targeting specific red flags.

VII. CONCLUSION

The unregulated state of defense offsets, combined with their many risk factors, make them especially vulnerable to corruption. Although there is currently no multinational consensus on how to regulate offsets, government regulation primarily through criminal statutes is insufficient. Offsets are government procurements, and as such countries providing and receiving offsets should affirmatively ensure they accomplish offset acquisitions without corruption. In addition, defense vendors should also heighten the urgency of their own compliance programs to further decrease offset corruption risks.

---

[371] Loughman & Sibery, *supra* note 47, at 145, 147.

[372] *Id.* at 144.

[373] *Id*. at 145.

[374] *Id*. at 151; Ernst & Young, *supra* note 44, at 24.

WIELDING A "VERY LONG, PEOPLE-INTENSIVE SPEAR": INHERENTLY GOVERNMENTAL FUNCTIONS AND THE ROLE OF CONTRACTORS IN U.S. DEPARTMENT OF DEFENSE UNMANNED AIRCRAFT SYSTEMS MISSIONS

*Major Keric D. Clanahan**

* Keric Dewey Clanahan, B.A., December 1992, Texas A&M University, M.A., December 1995, Texas A&M University, J.D., May 2007, Baylor Law School. The author wishes to thank Professors Steven L. Schooner and Laura A. Dickinson for their insight and guidance. He would also like to thank Mr. James (Ty) Hughes, Mr. Jim Ryan, Mr. Phillip H. Tritschler, Jr., Mr. Mike Shaughnessy, Mr. Matt Ullengren, Mr. Jeff Hurley, Colonel Kenneth Saunders, Lieutenant Colonel James J. Cutting, Lieutenant Colonel Chris "Otto" Recker, Major Casey Tidgewell, and Chief Master Sergeant Mark Kovalcik for sharing their experiences in the areas of Unmanned Aircraft Systems acquisitions, mission planning and operations, and systems support and training. Finally, he wishes to thank his wife, Cheryl, and children, Cole and Meghan, for their amazing love and support. The views expressed in this paper are solely those of the author and do not necessarily represent the views of DoD or its Components.

TABLE OF FIGURES

I. INTRODUCTION

A. Abstract

In the last decade of war, unmanned aircraft systems (UAS) have played a major role in the disruption of Al Qaeda, Taliban, and other insurgent enemy forces. Due to the lethality of these weapon systems, many critics have challenged the legality and morality of drone strikes. However, little scholarship has focused on the human capital requirements of the very diverse UAS mission, namely the personnel performing logistics and maintenance, video and imagery analysis, vehicle and sensor operation, and kinetic force delivery. This Article investigates the numerous roles necessary to sustain and perform the Department of Defense (DoD) UAS mission, and attempts to identify which roles are being performed by military, federal civilian, and/or civilian contractor personnel. Based on the nature of certain roles, this Article identifies rules that only Government personnel should perform certain activities because they are inherently governmental functions, or for other policy reasons. In conclusion, this Article provides recommended actions for both the DoD and Congress to ensure they avoid outsourcing certain inherently governmental UAS functions to contractors.

B. Introductory Case Study

Uruzgan Province, central Afghanistan, February 21, 2010, just a few hours before dawn.[1] A United States military special operations team, air dropped a few miles outside of the village of Khod, waits in the rugged mountain region getting ready for a raid to root out and capture insurgent forces suspected of operating in the area. Their mission is very similar to one the same team executed in the same district almost one year previously—on that day, firefights between U.S. military and insurgent forces erupted and one of our soldiers was killed. In 2009, the special ops team went in without any air support—in 2010, they have an AC-130 gunship, two Army Kiowa helicopters and a fully armed Predator unmanned aerial vehicle (UAV) watching over them.

[1] The following narrative is built upon investigative reports prepared by David S. Cloud of the *Los Angeles Times*; other news stories; and actual statements made by military members, federal civilians, defense contractors and Afghan local nationals to military investigators. *See generally* David S. Cloud, *Civilian Contractors Playing Key Roles in U.S. Drone Operations*, L.A. Times, Dec. 29, 2011 [hereinafter Cloud, *Civilian Contractors*], *available at* http://articles.latimes.com/print/2011/dec/29/world/la-fg-drones-civilians-20111230; NSI News Source Info, *U.S. Releases Uruzgan Investigation Findings ~ Afghanistan*, Def. Tech. News (May 30, 2010, 4:02 AM), *available at* http://defensenews-updates.blogspot.com/2010/05/dtn-news-us-releases-uruzgan.html; David S. Cloud, *Anatomy of an Afghan War Tragedy*, L.A. Times, Apr. 10, 2011, at A1, *available at* http://articles.latimes.com/2011/apr/10/world/la-fg-afghanistan-drone-20110410; Robert H. Reid, *U.S. Drone Crew Blamed for Afghan Civilian Deaths*, USA Today (Mar. 29, 2010), *available at* http://www.usatoday.com/news/topstories/2010-05-29-3963072919_x.htm.

Around 5:00 a.m. that morning, the AC-130 aircrew identifies a convoy of two sports utility vehicles (SUVs) and a pickup truck traveling along the dark mountain roads about seven miles away from, but heading toward, the team. At that moment, the American aircraft begin tracking the three vehicles. At 5:08 a.m., the AC-130 notices one of the vehicles flashing its headlights, and radios the information to the Creech Air Force Base (AFB), Nevada Predator flight crew, explaining that the vehicles appear to be sending signals. The Air Force pilot positions the Predator where it can best follow the vehicles; the Predator's cameras and sensors focus solely on the convoy. Back in Florida, a team of intelligence analysts and video screeners at Air Force Special Operations Command, Hurlburt Field, begin pouring over images as they are collected by Predator sensors. In real time, the screeners feed assessments to the Predator crew who are in communication with the ground force special operations team commander.

At 5:15 a.m., the Predator pilot thinks he identifies a rifle in one of the trucks; the camera operator concurs. The primary screener reports that her Florida team verifies about 20 military aged males (MAMs) with what appeared to be "possible weapons." The screener also reports the presence of possible children in the convoy. As the Predator continues tracking the vehicles, cell phone calls in the area are intercepted and translated. According to linguists providing intelligence support, the phone calls indicate that a Taliban unit is in the area preparing for an attack. Around 6:15 a.m., as dawn is breaking, the convoy stops. Several men exit the vehicles and begin unfolding what appear to be blankets, which they spread atop the nearby ground. The Predator crew watches as the men from the vehicles begin to pray. By 7:40 a.m., the screeners, after reviewing a couple of hours of fuzzy video, modify their report to the Predator crew and ground force commander: 21 MAMs, no females, and one adolescent—likely teenager.

With this last report from the screeners, the ground force commander concludes he has the positive identification necessary to engage a hostile force. By 8:40 a.m., the vehicles are driving away from the ground forces. Fearing a flanking maneuver, the ground force commander orders the Kiowas to stand ready for an attack. At 9:00 a.m., when the convoy reaches a section of open road, the ground commander calls for an airstrike. The aircraft unleash two Hellfire missiles that slam into the first and third vehicles, which burst into flames. Dead and wounded are everywhere. Very soon, the Nevada crewmembers and Florida screeners realize something has gone horribly wrong.

The investigation that soon followed would reveal that at least 15 Afghan civilians had been killed, to include one woman and three children, and 12 wounded. They were travelling together as a group for safety through the insurgent stronghold region of Uruzgan Province. Some were businessmen, others students returning to school, and a few were simply travelling to visit family. General Stanley McChrystal, then Commander of NATO and U.S. Forces, immediately offered his personal apologies to the people of Afghanistan and assured President Hamid Karzai that

actions would be taken against those who acted inappropriately, and that measures would be implemented to prevent similar accidents in the future. Four U.S. military officers—two who could be considered senior officers—were administered career-damaging letters of reprimands. No disciplinary action, however, was taken against the primary screener from Florida who provided imagery analysis that contributed to the decision to attack. There wasn't much that the military could do—she was a contractor.

C. Issue Preview

The Uruzgan Province incident raises numerous concerns about current U.S. military unmanned aircraft systems (UAS) missions, in particular, the role of contractors in UAS operations. Indeed, the role of contractors in military operations has been a subject of concern for several years. In the last decade alone, the United States spent hundreds of billions of dollars on contract support for military operations in Iraq and Afghanistan.[2] General concern over such expenses has been elevated to outrage in many through the discovery of the vast amount of taxpayer dollars that were lost to fraud, waste and abuse.[3] Defense contractors have been further disparaged in the press, academia and political circles for their involvement in activities many believe were not appropriate for contractors to perform. Serving as linguists and interrogators at the now infamous Iraqi Abu Ghraib prison, and as private security forces involved in the Nissour Square shooting deaths of Iraqi civilians, contractors were suddenly placed under intense scrutiny by the highest levels of government and the international community.[4] In short, there has been

---

[2] *See generally* Comm'n on Wartime Contracting in Iraq & Afghanistan, Transforming Wartime Contracting: Controlling Costs, Reducing Risks: Final Report to Congress (2011), [hereinafter CWC Final Report], *available at* http://www.wartimecontracting.gov/docs/CWC_FinalReport-lowres.pdf; Louis Peck, *America's $320 Billion Shadow Government*, The Fiscal Times (Sept. 28, 2011), http://www.thefiscaltimes.com/Articles/2011/09/28/Americas-320-Billion-Shadow-Government.aspx#page1; Moshe Schwartz, Wendy Ginsberg & Daniel Alexander, Cong. Research Serv., R41820, Department of Defense Trends in Overseas Contract Obligations (2011), *available at* http://www.fas.org/sgp/crs/misc/R41820.pdf; Moshe Schwartz & Joyprada Swain, Cong. Research Serv., R40764, Department of Defense Contractors in Afghanistan and Iraq: Background and Analysis (2011), *available at* http://www.d tic.mil/cgi-bin/GetTRDoc?AD=ADA543570.

[3] *See* CWC Final Report, *supra* note 2; Sharon Weinberger, *Windfalls of War: Pentagon's No-Bid Contracts Triple in 10 Years of War*, [hereinafter Weinberger, *Windfalls*], iWatch News, Aug. 29, 2011, *available at* http://www.iwatchnews.org/2011/08/29/5989/windfalls-war-pentagons-no-bid-contracts-triple-10-years-war; Charles S. Clark, *Pentagon contracting policy faulted in two reports*, Gov't Exec. (Aug. 29, 2011), *available at* http://www.govexec.com/oversight/2011/08/pentagon-contracting-policy-faulted-in-two-reports/34766/; Charles S. Clark, *IG: Iraq Logistics Contractor Marked Up Prices as Much as 12,000 Percent*, Gov't Exec. (Aug. 2, 2011), *available at* http://www.govexec.com/defense/2011/08/ig-iraq-logistics-contractor-marked-up-prices-as-much-as-12000-percent/34545/.

[4] *See generally* Mark Danner, Torture and Truth: America, Abu Ghraib, and the War on Terror (2004); Joe Davidson, *Defining Intelligence Contractors' Jobs, and Pay, is a Fuzzy Job*, Wash. Post, Sep. 20, 2011, *available at* http://www.washingtonpost.com/politics/column/feddiary/defining-intelligence-contractors-jobs-and-pay-is-a-fuzzy-job/2011/09/20/gIQAxNeWjK_story.html; Laura A. Dickinson, Outsourcing War & Peace: Preserving Public Values in a World of Privatized

resurgence of interest in pulling away from reliance on contractors for critical government missions. Any such insourcing, however, should not be reactionary, but rather performed in conjunction with a determination of the appropriate role of contractors during war. Such an evaluative approach would best serve our nation's military UAS mission.

While unmanned aircraft strike operations have generated a lot of criticism,[5] UAS undeniably have played a major role in the disruption of Al Qaeda, Taliban, and other insurgent enemy forces.[6] Unmanned technology has also been acknowledged as a weapons system that is truly saving American lives. Drones performing reconnaissance have detected numerous threats and improvised explosive devices (IEDs), protecting hundreds of our ground forces and convoys on maneuver.[7] And, it should go without saying, you do not have to worry about a downed pilot when a drone crashes. Important to hostile force identification and elimination, as well as force protection, the UAS mission is here to stay.

In the decade-long conflicts in Iraq and Afghanistan, the United States has used military troops, federal civilian employees and private military contractors to sustain and perform UAS missions. Now, after the end of the war in Iraq and entering the tenth year of war in Afghanistan, we must ask exactly what jobs are individuals performing in UAS operations? Who provides logistics and maintenance for unmanned aircraft? Who performs video and imagery analysis? Which individuals operate drones on strategic intelligence, tactical intelligence and targeted strike missions? And, most importantly, if private contractors are supporting

---

Foreign Affairs (2011) [hereinafter Dickinson, Outsourcing War & Peace]; Steven L. Schooner, *Contractor Atrocities at Abu Ghraib: Compromised Accountability in a Streamlined Outsourced Government*, 16 Stan. L. & Pol'y Rev. 549 (2005) [hereinafter Schooner, *Contractor Atrocities*]; P.W. Singer, *War, Profits, and the Vacuum of Law: Privatized Military Firms and International Law*, 42 Colum. J. Transnat'l L. 521 (2004); P.W. Singer, Corporate Warriors: The Rise of the Privatized Military Industry (2003).

[5] See *Infra* Part II.B (while a thorough analysis of the legality of unmanned strike operations is beyond the scope of this paper, Part II.B introduces many of the questions raised about UAV missions conducted in Pakistan and other nations); *see also* Paul McLeary, Sharon Weinberger & Angus Batey, *Drone War*, Aviation Wk. & Space Tech. (July 1, 2011), *available at* http://www.aviationweek.com/aw/generic/story_generic.jsp?channel=dti&id=news/dti/2011/07/01/DT_07_01_2011_p40-337605.xml&headline=Drone%20Impact%20On%20Pace%20Of%20War%20Draws%20Scrutiny; William S. Cohen, *Drones Can't Change War*, Politico *available at* http://www.politico.com/news/stories/0911/63927.html (last visited May 23, 2013,, 9:36 PM).

[6] *Infra* Part II.

[7] Kris Osborn, *U.S. Aviators, UAVs Team Up Against IEDs*, Def. News, Jan. 21, 2008, at 1, *available at* http://www.defensenews.com/story.php?i=3361963; Tim Owings, *Unmanned Aircraft Systems: The Intersection of the Army, available at* https://wiki.nps.edu/display/CRUSER/2011/11/28/Unmanned+Aircraft+Systems-+The+Intersection+of+the+Army (Feb. 1, 2012) (Tim Owings, Deputy Project Manager, Army Unmanned Aircraft Systems, writes "Maneuver units have grown to rely on the watchful "eye in the sky" unmanned aircraft to alert them to possible improvised explosive device emplacements and the massing of enemy forces and to provide battle damage assessment to ensure the success of recent missions.").

UAS missions, are they performing tasks that should be reserved exclusively for government personnel?

D. Chronology of Analysis

This article identifies numerous roles necessary to sustain and perform the Department of Defense (DoD) UAS mission, and finds that many of these roles should not be performed by contractors because they are inherently governmental functions, or for other policy reasons. Part I presents an introduction to analysis.

Part II provides an overview of the numerous UAS missions conducted by the U.S. Military and Central Intelligence Agency (CIA), the aircraft involved, and the activities and personnel requirements for the varied missions. Part III discusses the evolution of the policy and law regarding inherently governmental function, its most recent treatment in Office of Federal Procurement Policy (OFPP) Letter 11-1, *Performance of Inherently Governmental and Critical Functions*, and its relation to specific U.S. military regulations and International Humanitarian Law. Part III also establishes a framework that will be employed in my analysis of the UAS mission. Part IV analyzes the activities performed within the UAS mission to decide whether such activities should be considered inherently governmental and prohibited from contract performance, or while not inherently governmental, should still be performed by government personnel. The Article identifies, where data is available, activities contractors are currently performing. Of those activities, the Article identifies those that can continue to be performed by the private sector, and those that must, or should, be returned to government control. Part IV also discusses Law of Armed Conflict (LOAC) implications to civilian contractors and distinguishes the LOAC implications to contractors based on the roles contractors may perform related to UAS missions. Part V presents a number of recommendations for lawmakers to build internal UAS capability and prevent contractors from crossing the "inherently governmental" line. Part VI concludes by briefly discussing the advantages and disadvantages of alternative solutions, and concludes in favor of the recommended solutions.

II. BACKGROUND: UNMANNED AIRCRAFT SYSTEMS

Until recently, many would have remarked that Unmanned Aircraft Systems (UAS)—often referred to as Unmanned Aerial Vehicles (UAVs), Remotely Piloted Aircraft (RPAs), or the more widely known and pejorative term, Drones[8]—were

[8] It is important to note that there is a crucial difference between the terms UAV, RPA, and drone and the term UAS. The first three terms refer to individual aircraft, while the term UAS refers to an aggregation of ground equipment, information technology and multiple aircraft. Department of Defense, Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, Nov. 8, 2010 (as amended Nov. 15, 2011) [hereinafter JP 1-02], at 359, defines "unmanned aircraft" as "[a]n aircraft or balloon that does not carry a human operator and is capable of flight under remote control or autonomous programming," "unmanned aircraft system" as "[t]hat system

built to be targets that real pilots shot down for practice, or maybe model planes you could fly into secured airspace to get a few helpful pictures. In contrast, it took real planes flown by real pilots to put bombs on target.[9] Undeniably, UAS technology has made incredible contributions to the Global War on Terrorism being waged in Iraq and Afghanistan.[10] In fact, in this age of armed conflict against non-state adversaries and ongoing counterinsurgency operations, UAS may be the most effective weapon employed at this time,[11] ultimately proving itself as the linchpin technology for the detection, identification and ultimate elimination of key leaders within the Taliban and al Qaeda, including Osama bin Laden.[12]

A. The Growth of Unmanned Systems

UAVs in military service today are the result of an erratic history. The first remotely piloted UAVs emerged during World War I, securing initial military backing for wartime production.[13] However, with governmental support and funding quickly waning, the Army shifted its focus to the development of piloted aircraft technology. Radio-controlled aircraft technology lost its place in the military arsenal, and was sidelined to the world of toys.[14] Ironically, the excitement and innovation of remote-controlled aircraft enthusiasts would drive the development of what would evolve into some of the United States' most effective, lethal weapons. UAVs reemerged as a technology of interest when the intelligence community recognized such aircraft as vital tools for getting behind the Soviet Iron Curtain and into China to collect

---

whose components include the necessary equipment, network, and personnel to control an unmanned aircraft."

[9] *See generally* Bill Yenne, Birds of Prey: Predators, Reapers and America's Newest UAVs in Combat 71 (2010).

[10] Despite the success of the UAS as an intelligence asset and as weapons systems, there exist many within the military services who remain highly critical. See, for example, highly critical online posts made by military pilots on AV Web, http://www.avweb.com/blogs/insider/AvWebInsider_Drones_202180-1.html (May 23, 2013 at 1:32 a.m.), or CBS News, *available at* http://www.cbsnews.com/8618-100_162-4540269.html?assetTypeId=30&messageId=7292805 (last visited May 23, 2013 at 1:35 a.m.).

[11] Christopher Drew, *For U.S., Drones Are Weapons of Choice in Fighting Qaeda*, N.Y. Times, Mar. 17, 2009, at A1, *available at* http://www.nytimes.com/2009/03/17/business/17uav.html?pagewanted=all (writing that Pentagon officials claim UAVs "have done more than any other weapons system to track down insurgents and save American lives in Iraq and Afghanistan.")

[12] Stuart Fox, *Hi-Tech Surveillance Plus Old-Fashioned Intelligence Work Found Osama Bin Laden,* InnovationNewsDaily (May 2, 2011), *available at* http://www.innovationnewsdaily.com/osama-death-surveillance-predator-drone-wiretap-1946/; Mark Mazzetti, *C.I.A. Drone Is Said to Kill Qaeda's No. 2*, N.Y. Times, Aug. 28, 2011, at 1, *available at* http://www.nytimes.com/2011/08/28/world/asia/28qaeda.html?_r=1.

[13] Yenne, *supra*, note 9, at 9 (several inventors in the U.S. and Europe produced radio and television controlled aircraft and rockets during World War I. Notably, the Delco company produced a recoverable aircraft with a 60-mile range, for which it was awarded a contract with the U.S. Army to produce what were intended to serve as "precursors to modern cruise missiles." When the war ended, the program was cancelled.)

[14] *Id.*

valuable pictures and information.[15] With success with the new spy mission, the Federal Government funded production of numerous unmanned aircraft. These were deployed to support military intelligence, surveillance, and reconnaissance (ISR) needs in Vietnam,[16] Bosnia and Kosovo,[17] and the first Gulf War.[18] The U.S., however, was not the only country to recognize the value of unmanned technology. Great Britain, France, Germany, Canada, Israel, South Korea, Demark, Sweden, India, China and Iran all made substantial investments in UAV technology.[19] In fact, throughout the 1990s and 2000s, Israel led all other nations in unmanned technology development and military utilization.[20] Since then, however, many nations, particularly the United States, have dramatically advanced unmanned technology development and production for weapon systems as well as non-military applications.[21]

---

[15] *Id.* at 13-17; For a very thorough history of the development of UAVs, *see generally* Thomas P. Ehrhard, The Mitchell Institute for Airpower Studies, *Air Force UAVs: The Secret History*, Jul. 2010, at 5, *available at* http://www.afa.org/mitchell/reports/MS_UAV_0710.pdf ("The US intelligence community is the single greatest contributor to US operational UAV development. Over the span of this study—roughly, 1960 through 2000—the intelligence community budget funded more than 40 percent of the total US UAV investment, double that of the next greatest contributor.")

[16] Yenne, *supra* note 9, at 13-17; Ehrhard, *supra*, note 15, at 23-29 (During the Vietnam War, "Air Force drones flew more than 3,500 combat sorties in a wide variety of roles, prompting the Air Force to make a major commitment to UAV development in the early 1970s.")

[17] Ehrhard, *supra*, note 15, at 50; Office of the Secretary of Defense (OSD), *FY2009-2034 Unmanned Systems Integrated Roadmap* (April 2009) [hereinafter *Integrated Roadmap*], at 63, *available at* http://www.acq.osd.mil/psa/docs/UMSIntegratedRoadmap2009.pdf.

[18] Ehrhard, *supra*, note 15, at 25 (describing the use of 40 Chukar target drones as data gatherers and decoys during the first two days of the Gulf War).

[19] *See generally Rise of the Drones: Unmanned Systems and the Future of War, Hearing before the House Subcomm on Nat'l Sec. and Foreign Affairs*, 11th Cong. (Mar. 23, 2010) [hereinafter *Rise of the Drones I*]; Chris Jenks, *Law from Above: Unmanned Aerial Systems, Use of Force, and the Law of Armed Conflict*, 85 N.D. L. Rev. 649 (2009); Robert Sparrow, *Building a Better WarBot: Ethical Issues in the Design of Unmanned Systems for Military Applications*, 15 Sci. Eng. Ethics 169, 170 (2009); Peter Singer, *Military Robots and the Laws of War*, The New Atlantis 27 (2009).

[20] *See* Tony Rock, Y*esterday's Laws, Tomorrow's Technology: the Laws of War and Unmanned Warfare*, 24 N.Y. Int'l L. Rev. 39, 41 (2011) (citing Mark Edward Peterson, *The UAV and the Current and Future Regulatory Construct for Integration into the National Airspace System*, 71 J. Air L. & Com. 521, 545-46 (2006) ("stating that the Israeli Defense Forces were further ahead in the development and usage of UAVs compared to other countries"); Ralph Sanders, *An Israeli Military Innovation: UAVs*, 33 Joint Force Q. 114 (2002) ("crediting Israel with the maturity of UAVs to their current status despite other countries' experimentation with the systems"); and J. Ricou Heaton, *Civilians at War: Reexamining the Status of Civilians Accompanying the Armed Forces*, 57 A.F. L. Rev. 155, 168 (2005) (referencing "Israel's use of UAVs in Lebanon during 1982 for the purpose of destroying Syrian technology.")).

[21] *See generally* Tom Brown, *Spy-in-the-Sky Drone Sets Sights on Miami*, Reuters, *available at* http://www.reuters.com/article/2008/03/26/us-usa-security-drones-idUSN1929797920080326 (describing Miami-Dade plans to utilize UAVs for local law enforcement) Mar. 30, 2008; Eric Lipton, Bush Turns to Big Military Contractors for Border Patrol, N.Y. Times, May 18, 2006, *available at* http://www.nytimes.com/2006/05/18/washington/18border.html?pagewanted=print (discussing plans originating in 2006 to use UAVs to assist Department of Homeland Security, Customs and Border Protection division, monitoring and patrol of 6,000 miles of border land); Edward D. McCormack,

B. Recent Media Attention

Most attention given to UAVs in the past few years has focused on the targeted strike missions that have occurred principally in Pakistan, with some missions engaging targets in Yemen or Libya. Regarded by many as the worst kept secret in the intelligence community,[22] the unacknowledged CIA program has generated a considerable amount of applause and criticism. Hailed by many as America's most effective weapon against terrorist organizations,[23] UAVs have been used to eliminate at least 67 Taliban and al Qaeda senior leaders and commanders, and thousands of terrorist operatives, in Pakistan alone.[24] Advocates argue that

---

The Use of Small Unmanned Aircraft by the Washington State Department of Transportation, Report Prepared for the Washington State Transportation Commission, Department of Transportation, June 2008 (engineering feasibility study of the proposed use of UAVs as an "avalanche control tool on mountain slopes above state highways); *Rise of the Drones I, supra* note 19 (statement of Michael Fagan, Chair, Association for Unmanned Vehicle Systems International (AUVSI), addressing the non-military uses of unmanned systems, the need for greater access to the national airspace, and projected future use of UAVs for combating piracy, law enforcement, border patrol, emergency response, wildfire monitoring, monitoring civil unrest, search and rescue, port security, submarine detection, underwater mine clearance, land mine and IED removal, fish tracking, and aerial photography).

[22] *See generally* David Fulghum, *The CIA's Air Force Is Back in Operation*, Aviation Week, 2005, *available at* http://www.aviationweek.com/aw/jsp_includes/articlePrint.jsp?headLine=The%20CIA's%20Air%20Force%20Is%20Back%20in%20Operation&storyID=news/02285p01.xml (describing the reports of the CIA conducting unmanned intelligence missions over Iran in 2005); Scott Shane, *C.I.A. to Expand Use of Drones in Pakistan*, N.Y. Times, Dec. 3, 2009, *available at* http://www.nytimes.com/2009/12/04/world/asia/04drones.html?ref=unmannedaerialvehicles (describing White House expansion of the C.I.A.'s UAV program in Pakistan's lawless tribal areas, at same time Administration announced deployment of an additional 30,000 troops to Afghanistan); Julian E. Barnes, *Panetta Makes Cracks About Not-So-Secret CIA Drone Program*, Wall St. J., Oct. 7, 2011, *available at* http://blogs.wsj.com/washwire/2011/10/07/panetta-makes-cracks-about-not-so-secret-cia-drone-program/ (quoting former CIA director, present Defense Secretary, Leon Panetta: "Having moved from the CIA to the Pentagon, obviously I have a hell of a lot more weapons available to me in this job than I had in the CIA, although the Predators weren't bad.").

[23] *See e.g.,* Peter Taylor, *Drones 'winning' war against al-Qaeda, says ex-CIA head*, BBC News World, Mar. 20, 2011, *available at* http://www.bbc.co.uk/news/world-12784129; Sadanand Dhume, *In Praise of Drones: The Case for Using Armed Unmanned Aerial Vehicles in Pakistan is Stronger Than Ever*, Wall St. J. Online, Aug. 18, 2011, *available at* http://online.wsj.com/article/SB10001424053111903639404576513734002079242.html.

[24] *The Long War Journal*, the product of the Foundation for Defense of Democracies and journalists Bill Roggio and Thomas Joscelyn, provides what is widely regarded as one of the most accurate tracking reports of the UAV strike mission in Pakistan. From 2004 through November 17, 2011, they report 279 strikes have taken place—269 occurring since January 2008. According to *The Long War Journal*, approximately 2,150 leaders and operatives from Taliban, Al Qaeda, and allied extremist groups have been killed since 2006. And, while many organizations opposing the UAV strike program have claimed that thousands of innocent civilians have been killed, *The Long War Journal* states that reports received "from reporters in the field, existing news and wire reports, and confidential and public sources" indicate that 138 Pakistani civilians have been killed since 2006. For more information, *see* http://www.longwarjournal.org/. Another insightful investigation conducted by the New America Foundation, finds similar results: "Our study shows that the 283 reported drone strikes in northwest Pakistan, including 70 in 2011, from 2004 to the present have killed approximately between 1,717 and 2,680 individuals, of whom around 1,424 to 2,209 were described as militants in reliable press accounts. Thus, the true non-militant fatality rate since 2004

the UAV strikes are a legitimate, justified mission based upon a broader, but more widely accepted, principle of self-defense that has arisen in the post-September 11 age of asymmetric warfare.[25] However, many politicians, scholars, and diplomatic representatives have criticized the CIA program severely—some actually accusing the U.S. of committing international war crimes and extrajudicial killings.[26] In brief, opponents levy the charges that (1) targeted strikes potentially violate the law of war principle of distinction by targeting locations largely populated by civilians rather

---

according to our analysis is approximately 17 percent. In 2010, it was more like five percent." For more information, *see* http://counterterrorism.newamerica.net/drones.

[25] *See e.g.,* Harold Hongju Koh, Legal Advisor, U.S. Dep't of State, Address at the Annual Meeting of the American Society of International Law, *The Obama Administration and International Law* (Mar. 25, 2010), *available at* http://www.state.gov/s/l/releases/remarks/139119.htm (last visited Jan. 16, 2012) (stating that the Obama administration has carefully reviewed unmanned targeting operations to ensure that strike missions comply with the laws of war—limited to only military objectives, avoided where civilian damage is excessive in relation to military advantage, conducted as legitimate self defense of a state in armed conflict, and not constituting assassination). *See also* Kenneth Anderson, *Targeted Killing in U.S. Counterterrorism Strategy and Law: A Working Paper of the Series on Counterterrorism and American Statutory Law, a joint project of the Brookings Institution, the Georgetown University Law Center, and the Hoover Institution* (May 11, 2009), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1415070 (arguing that unmanned targeted strikes, as used in the current international conflict, are justified self-defense against terrorist organizations, but cautioning that "careful and assertive legal steps" are required to prepare for the possible use of unmanned weapons against groups not "covered by Security Council resolutions or the US Authorization for the Use of Military Force").

[26] Much journalism and scholarship has been devoted to the growing use of UAS to conduct targeted strikes against al Qaeda and Taliban leadership in Pakistan, Yemen, and Libya. Although the CIA is recognized as conducting these missions, CIA direction and execution has not been officially recognized. This paper primarily examines the role of private contractors in our nation's previous and current UAS mission in Iraq and Afghanistan. While the role of contractors is considered in strikes conducted in Pakistan, Yemen or Libya, this paper does not attempt to fully address the legality of the target strike operations. For more information regarding international and domestic legal issues surrounding justifications for and protests of target strikes, *see generally id*.; Laurie R. Blank & Benjamin R. Farley, *Characterizing U.S. Operations in Pakistan: Is the United States Engaged in an Armed Conflict?*, 34 Fordham Int'l L.J. 151 (2010); Peter Finn, *A Future for Drones: Automated Killing*, Wash. Post, Sep. 19, 2011, *available at* http://www.washingtonpost.com/national/national-security/a-future-for-drones-automated-killing/2011/09/15/gIQAVy9mgK_story.html; Victor Hansen, *Predator Drone Attacks*, 46 New England L. Rev 27 (2011); Greg Miller & Julie Tate, *CIA Shifts Focus to Killing Targets*, Wash. Post, Sep. 1, 2011, *available at* http://www.washingtonpost.com/world/national-security/cia-shifts-focus-to-killing-targets/2011/08/30/gIQA7MZGvJ_story.html; Mary Ellen O'Connell, *The Choice of Law Against Terrorism*, 4 J. Nat'l Sec. L. & Pol'y 343 (2010); *Rise of the Drones II, Examining the Legality of Unmanned Targeting: Hearing Before the Subcomm. on Nat'l Sec. and Foreign Affairs of the H. Comm. on Oversight and Gov't Reform,* 111th Cong. 1–2 (2010) [hereinafter *Drones II Hearing*] *available at* http://oversight.house.gov/index.php?option=com_content&view=article&id=681%3A04-28-2010-qrise-of-the-drones-ii-examining-the-legality-of-unmanned-targetingq&catid=17&Itemid=1; Afsheen John Radsen & Richard Murphy, *Measure Twice, Shoot Once: Higher Care For CIA-Targeted Killing*, 4 U. Ill. L. Rev. 1201 (2011); Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, *Study on Targeted Killings,* ¶¶ 53-56, U.N. Doc. A/HRC/14/24/Add.6 (May 28, 2010) (by Philip Alston), *available at* http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.24.Add6.pdf.

than legitimate military objects;[27] (2) that the targets are not legitimate military targets but rather criminals who should be subjected to law enforcement procedures,[28] and (3) that the CIA, a civilian agency, is unlawfully conducting military operations that should be reserved for the U.S. armed forces.[29]

Although much attention has been focused on the legality of CIA targeted strike operations, the general public has paid little attention to the broad array of UAS currently in service with, or in development for, the Department of Defense. Except for followers of military and aviation media, most peoples' exposure to UAS is likely limited to the pictures they have seen in USA Today, reports on CNN, or bootlegged videos uploaded to YouTube. In other words, when people think of UAS, they likely envision MQ-1 Predators shooting Hellfire missiles. In response, the DoD UAS universe involves much more. This Article will introduce the reader to the primary aircraft, ground systems, and personnel—military, federal civilian and private contractor—involved in U.S. armed forces UAS missions.

C. Primary Unmanned Aircraft Systems, Missions, and Operations

The Department of Defense's recognition of the UAS warfighting capability led to a surge in its development, acquisition, and deployment. Asked at a 2005 Congressional hearing how many MQ-1 Predator unmanned aircraft his service needed for the next fiscal year, former Air Force Chief of Staff General John P. Jumper responded, "We're going to tell General Atomics [the California based manufacturer] to build every Predator they can possibly build."[30] Industry quickly acted upon this enthusiasm, which spread throughout all of the military services: from 2002 through 2011, the U.S. inventory of unmanned aircraft exploded from 167 to over 7000 for all the military branches, the majority of this inventory being small, short-range reconnaissance aircraft.[31] The DoD inventory consists of UAVs of

---

[27] *See e.g.,* Jonathan Masters, Council on Foreign Relations, *Targeted Killings*, Nov. 7, 2011, *available at* http://www.cfr.org/intelligence/targeted-killings/p9627; Murtaza Hussain, *Pakistan's Legal Fight to End the Drone War,* Aljazeera, Dec. 15, 2011, *available at* http://www.aljazeera.com/indepth/opinion/2011/12/20111213112743546541.html; Laurie Blank, *Drone Strike Casualties and the Laws of War*, JURIST - Forum, Aug. 22, 2011, *available at* http://jurist.org/forum/2011/08/laurie-blank-drone-strikes.php.

[28] *See e.g.,* Glenn Greenwald, *The We-Are-At-War Mentality*, Salon, Dec. 3, 2011, *available at* http://www.salon.com/2011/12/03/the_we_are_at_war_mentality/; Thomas R. Eddlem, *Awlaki Killing: Does America Need Courts, Juries, or Trials Anymore?*, The New American, Oct. 1, 2011, *available at* http://thenewamerican.com/usnews/constitution/9220-awlaki-killing-does-america-need-courts-juries-or-trials-any-more.

[29] *See e.g.,* Morris Davis, *Combatant Immunity and the Death of Anwar al-Awlaqi*, JURIST - Forum, Oct. 17, 2011, *available at* http://jurist.org/forum/2011/10/morris-davis-anwar-al-awlaqi.php; Keith Johnson, *U.S. Defends Legality of Killing with Drones*, Wall St. J., Apr. 5, 2010, *available at* http://online.wsj.com/article/SB10001424052702303450704575159864237752180.html.

[30] Joseph C. Anselmo, *Build It and They Will Come*, Aviation Wk. & Space Tech., May 29, 2005, *available at* http://www.aviationweek.com/aw/generic/story_generic.jsp?channel=awst&id=news/05305p01.xml.

[31] P.W. Singer, *Unmanned Systems and Robotic War*, Mar. 23, 2010; *available at* http://www.

various types, sizes and capabilities, ranging from the 10-inch long, 1-pound Wasp III to the 15,000 lbs RQ-4B Global Hawk with its 131 foot wingspan.[32] Moreover, even with an already impressive arsenal, the DoD does not appear to be slowing down the purchase of UAS anytime soon. In its FY 2012 *Program Acquisition Costs by Weapon System* budget request, the DoD identified $54.2 Billion as the required funding to support all aircraft acquisitions, $3.88 Billion of that just for UAS.[33]

1. Large and Medium Unmanned Systems

The two largest unmanned aircraft in the military inventory are Air Force RQ-4B Global Hawk and the Navy Broad Area Maritime Surveillance (BAMS) aircraft, which are variants of the same Northrop Grumman aircraft.[34] Classified as Group 5 UAS, the latest versions of the aircraft are the size of small commercial jet, with a wingspan of 131 feet with a body length 48 feet.[35] Not armed, the two UAS are built to operate up to 60,000 feet in altitude and serve as theater-wide ISR (intelligence-surveillance-reconnaissance) platforms, complementing manned and space ISR systems.[36] The Global Hawk's principle "mission is to provide a broad spectrum of ISR collection capability to support joint combatant forces in

brookings.edu/testimony/2010/0323_unmanned_systems_singer.aspx (article presenting Dr. Singer's testimony before the U.S. House of Representatives Committee on Oversight and Government Reform, Subcommittee on National Security and Foreign Affairs regarding the colossal growth of the robotics industry and the necessity of U.S. policy and law staying engaged); U.S. Gov't Accountability Office, GAO-09-520, Defense Acquisitions: Opportunities Exist to Achieve Greater Commonality and Efficiencies among Unmanned Aircraft Systems 5 (2009), *available at* http://www.gao.gov/new.items/d09520.pdf (suggesting that, although all military branches began large scale acquisitions of unmanned aircraft, greater advantages may have been achieved through more cooperative, joint weapons systems development).

[32] Dep't of the Air Force, U.S. Air Force Fact Sheet: Wasp III (2013), http://www.af.mil/information/factsheets/factsheet.asp?fsID=10469 [hereinafter Wasp III Fact Sheet]; Dep't of the Air Force, U.S. Air Force Fact Sheet: RQ-4 Global Hawk (2012), http://www.af.mil/information/factsheets/factsheet.asp?fsID=13225 [hereinafter Global Hawk Fact Sheet].

[33] Office of the Under Secretary of Defense (Comptroller)/CFO, United States Department of Defense, Fiscal Year 2012 Budget Request: Program Acquisition Costs by Weapons System (2011), at 1-1, *available at* http://comptroller.defense.gov/defbudget/fy2012/FY2012_Weapons.pdf.

[34] GAO-09-520, *supra* note 31, at 14-16 (The GAO criticized military services' efforts in large scale acquisitions of unmanned aircraft, stating that greater advantages would have been achieved through more cooperative, joint weapons systems development. GAO did applaud the Navy for adopting the RQ-4B as the foundational aircraft upon which the BAMS would be developed, but noted that greater efficiencies would have been possible through more commonality in sensor acquisition).

[35] Cong. Budget Office, Policy Options for Unmanned Aircraft Systems, Pub. No. 4083, at 4 (2011), *available at* http://www.cbo.gov/doc.cfm?index=12163 [hereinafter CBO Policy Options].

[36] *Id.* at 2-4.

worldwide peacetime, contingency, and wartime operations,"[37] while the BAMS' primary function is persistent maritime ISR.[38]

The only other Group 5 UAS[39] is the Air Force MQ-9 Reaper, "an armed, multi-mission, medium-altitude, long endurance remotely piloted aircraft (RPA) that is employed primarily in a hunter/killer role against dynamic execution targets and secondarily as an intelligence collection asset."[40] Proposed by the Air Force after the successes realized with weaponized MQ-1 Predators, the Reaper (formerly Predator-B) was produced by General Atomics as a follow-on UAV with upgraded capabilities.[41] Thirteen feet longer with a 16-foot greater wingspan, powered by a 900hp turboprop engine, and able to carry up to 16 Hellfire missiles or "a mix of 500-pound weapons and Small Diameter Bombs"[42]—the Reaper could be thought of as the Predator's super tough, big brother.

UAVs considered medium sized, or Group 4, are the most commonly known to the world, since the class includes the MQ-1 Predator, the primary strike vehicle used in the last decade. Also regarded as medium size UAVs are the MQ-1C

---

[37] Global Hawk Fact Sheet, *supra* note 32 (The Global Hawk is regarded as one of the oldest and most important UAS in the DoD inventory: "Global Hawk began as an Advanced Concept Technology Demonstration in 1995. The system was determined to have military utility and provide warfighters with an evolutionary high-altitude, long-endurance ISR capability. While still a developmental system, the Global Hawk deployed operationally to support the global war on terrorism in November 2001. The Global Hawk UAS provides near-continuous all-weather, day/night, wide area reconnaissance and surveillance.").

[38] BAMS UAS Program Office Description, *available at* http://www.navair.navy.mil/index.cfm?fuseaction=home.displayPlatform&key=F685F52A-DAB8-43F4-B604-47425A4166F1, last visited Jan. 16, 2012.

[39] While technically not recognized as a Group 5 UAS, the RQ-170 Sentinel meets the requirements based on 65-foot wingspan and likely flight ceiling capacity. The Air Force currently possesses an undisclosed quantity of RQ-170 Sentinels, a classified stealth reconnaissance aircraft, for which the service only acknowledged existence until the aircraft gained recent notoriety after going down while over Iranian airspace. *See generally* Dep't of the Air Force, U.S. Air Force Fact Sheet: RQ-170 Sentinel (2011), http://www.af.mil/information/factsheets/factsheet.asp?fsID=16001; John Walcott, *Iran Shows Off Downed Spy Drone as U.S. Assesses Technology Loss*, Bloomberg Bus. Wk. (Dec. 10, 2011), *available at* http://www.businessweek.com/news/2011-12-10/iran-shows-downed-spy-drone-as-u-s-assesses-technology-loss.html (recounting that the RQ-170 went down, allegedly due to an undisclosed malfunction, which led to the technology falling into the hands of the Iranians.).

[40] Dep't of the Air Force, U.S. Air Force Fact Sheet: MQ-9 Reaper (2012), *available at* http://www.af.mil/information/factsheets/factsheet.asp?fsID=6405.

[41] *See* David Crane, *MQ-9 Predator-B 'Hunter-Killer' UCAV Gets a New Name: Meet the Reaper*, Defense Review (Sep. 20, 2006), *available at* http://www.defensereview.com/mq-9-predator-b-hunter-killer-ucav-gets-a-new-name-meet-the-reaper/.

[42] *Id.*; Jeremiah Gertler, Cong. Research Serv., R42136, *U.S. Unmanned Aerial Systems* (2012), at 35, *available at* http://fpc.state.gov/documents/organization/180677.pdf (Stating that "DOD's unmanned aircraft inventory increased more than 40-fold from 2002 to 2010"); Lt. Col Christophe F. Roach, *Robots in the Sky—The Legal Effects and Impacts of UAV on the Operational Commander*, at 4-5 (October 31, 2008) (paper submitted to the Naval War College in partial satisfaction of requirements, noting that the MQ-9 Reaper has the same armament capability as an F-16 fighter, but adds additional persistence to force contribution since it can remain in an area for 18-20 hours).

Gray Eagle, the MQ-5B Hunter, and the MQ-8B Fire Scout, the Navy's unmanned helicopter.[43] The Air Force Predator is 27 feet long, with a 55 foot wingspan, and capable of carrying both ISR sensors and 2 Hellfire missiles. In comparison, the Army developed a variant, the MQ-1C Gray Eagle, which is slightly longer, wider, outfitted with an alternate sensor configuration, and capable of carrying up to 4 Hellfires.[44] The MQ-5B Hunter is a nearly 2,000 lb. tactical ISR vehicle, with a wingspan of 34 feet, and the capability to be armed with anti-tank munitions.[45] The MQ-8B Fire Scout is the first unmanned helicopter developed and deployed to support joint operations.[46] Presently unarmed and conducting ISR and target acquisition missions, the Navy has experimented with weaponizing the helicopter, and plans to add missiles to future aircraft.[47]

2. Small and Micro Unmanned Systems

The majority of the U.S. armed forces' UAS inventory consists of micro-sized to small systems, categorized as Groups 1-3 small UAS (SUAS).[48] The principle SUAS employed by the military include the RQ-7 Shadow, Scan Eagle, RQ-11 Raven, Wasp, Puma AECV, gMAV/T-Hawk, and Switchblade.[49] Called the Army's tactical "workhorse,"[50] the RQ-7 Shadow is a rail-launched UAV that

---

[43] CBO Policy Options, *supra* note 35, at viii.

[44] GAO-09-520, *supra* note 31, at 16-18 (GAO sternly criticized the inability of the Air Force and Army to work together since 2001 to achieve commonalities in requirements for the next generation of UAVs. Unable to reach agreement on the questions of control stations, sensor capabilities, and armaments, the Air Force and Army have developed 3 different UAV programs, for similar systems (Predator, Reaper, and Gray Eagle (formerly, Sky Warrior)) from the same manufacturer, General Atomics).

[45] Gertler, *supra* note 42, at 42; U.S. Army UAS Center of Excellence, *"Eyes of the Army," U.S. Army Roadmap for Unmanned Aircraft Systems*, 2010-2035 (2010), at 77, *available at* http://www.aviationweek.com/media/pdf/UnmannedHorizons/US%20Army%20UAS%20RoadMap%202010%202035.pdf [hereinafter Army Roadmap].

[46] Gertler, *supra* note 42, at 40-41.

[47] *Id.; but see Navy's Fire Scout Fleet Not Grounded, Only Curtailed*, Nat'l Def., Apr. 2012, *available at* http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=755 (reporting that the Navy has temporarily suspended flying missions for the MQ-8B Fire Scout to investigate "two unrelated crashes," but has authorized commanders to use the UAV if operationally necessary).

[48] As of January 2012, the total inventory of military SUAS was just over 7,000 aircraft. *See* Gertler, *supra* note 42, at 8.

[49] *Id.; see also* Eric Beidel, *Military Investigates Killer Drones That Can Fit in Rucksacks*, Nat'l Def., Jul. 2011, *available at* http://www.nationaldefensemagazine.org/archive/2011/July/Pages/MilitaryInvestigatesKillerDronesThatCanFitinRucksacks.aspx (describing the Switchblade, the Army's initial lethal miniature aerial munitions system (LMAMS)); for brief descriptions and photographs of the numerous SUAS in use by the United States and other nations, *see* Popular Science *Gallery: The Complete UAV Field Guide, available at* http://www.popsci.com/technology/gallery/2010-02/gallery-future-drones.

[50] Army Roadmap, *supra* note 45, at 55 ("As a fully integrated, organic asset, the RQ-7C provides the ground commander with tactically significant situational awareness and the ability to influence operations in a timely manner.").

is 11 feet long, with a 14-foot wingspan, and capable of climbing to 14,000 feet.[51] Currently unarmed, although outfitted with a laser designator for targeting, the Shadow is being modified for the Marines to carry weapons.[52] Other SUAS, such as the Scan Eagle, Wasp and RQ-11 Raven, are flown for tactical reconnaissance, surveillance and target acquisition, mainly supporting force protection and special operations.[53] The gMAV/T-Hawk is quite unique—a small little hovercraft shaped like an outdoor barbecue, the SUAS adds vital capabilities to the explosive ordnance disposal (EOD) mission.[54] The Switchblade differs from its brethren because the aircraft itself is intended to be a disposable munition. Compared to the Kamikazes that devastated the U. S. Pacific Fleet at Pearl Harbor, the Switchblade can be taken out of a rucksack, tossed into the air, guided remotely toward a hostile force, and then flown directly into the target where it explodes upon impact.[55] Unlike the Predator, Reaper and Global Hawk aircraft, SUAS do not employ the remote-split operation described in the following section. Rather, SUAS are controlled by individuals on the ground in the area of conflict, who typically have access to a live video feed provided by the drone of the areas and/or individuals being surveyed or targeted.[56] In the recent past, both military and contractor personnel have operated many of these weapons systems.[57]

---

[51] Gertler, *supra* note 42, at 43-44; Army Roadmap, *supra* note 45, at 76.

[52] *Id.*; Interview of Lieutenant Colonel James J. Cutting, Headquarters, Department of the Army, Operations, Plans, and Training (Unmanned Aviation), HQDA DCS G-3/5/7, Jan. 6, 2012 [hereinafter Lt Col Cutting Interview] (stating that the Army was currently engineering the weapons capability for the Marine Corps, but the weaponized Shadow had not yet been fielded. If the armed Shadow proves successful for the Marines, the Army likely will move ahead with a similar modification of its inventory); Staff Writers, *Arming RQ-7 UAVs: The Shadow Knows…*, Def. Industry Daily, Jan. 15, 2012, *available at* http://www.defenseindustrydaily.com/Mortars-from-Aircraft-The-Shadow-Knows-05226/ (describing the challenges of adding firepower to small tactical UAVs).

[53] Dep't of the Air Force, U.S. Air Force Fact Sheet: Scan Eagle (2011), http://www.af.mil/information/factsheets/factsheet.asp?id=10468; Wasp III Fact Sheet, *supra* note 32; Dep't of the Air Force, U.S. Air Force Fact Sheet: RQ-11B Raven (2011), http://www.af.mil/information/factsheets/factsheet.asp?id=10446 [hereinafter Raven Fact Sheet].

[54] David Eshel, Mini-UAVs rack up big gains, Def. Tech. Int'l, May 15, 2008, *available at* http://integrator.hanscom.af.mil/2008/May/05222008/05222008-17.htm (writing that the gMAV/T-Hawk has become an important asset to the Army and Marines ground troops because of "its ability to inspect a target—a suspicious vehicle, structure or disturbed earth—from close range, covering ground much more quickly than an unmanned ground vehicle and without putting people at risk").

[55] Beidel, *supra* note 49.

[56] *Id.*

[57] *Id.*; U.S. Gov't Accountability Office, GAO-09-175, Unmanned Aircraft Systems: Additional Actions Needed to Improve Mgmt. and Integration of DOD Efforts to Support Warfighter Needs 7 (2008) [hereinafter GAO Additional Actions], *available at* http://www.gao.gov/assets/290/283271.pdf (GAO reports that the Army used contractors to operate the gMAV, Hunter, I-Gnat, and Warrior-Alpha UAS. The Air Force used contractor operators for Scan Eagle missions); Bill Sweetman, *Contractors Make UAV Ops Happen*, Aviation Week, Dec. 1, 2009, *available at* http://www.aviationweek.com/aw/generic/story.jsp?id=news/UAVs120109.xml&headline=ContractorsMakeUAVOpsHappen&channel=defense (Reporting the Army's use of contractors to operate I-Gnat UAS and the Marines contracting Scan Eagle operations.)

3. Remote-Split Operations

Perhaps the most revolutionary—and possibly most criticized—aspect of UAS technology is the capability it provides to fight in war without having to actually be present.[58] Referred to as remote-split operations (RSO), the Air Force devised a centralized management and execution strategy for UAS missions: RSO pilots, operators and intelligence personnel remain stateside at the Creech Air Force Base, Nevada, Global Operations Center, Nevada, or other regional centers, while a smaller contingent of personnel are deployed to the theater of war to handle launch and recovery.[59] According to Lieutenant General Dave Deptula, Air Force Deputy Chief of Staff, Intelligence, Surveillance and Reconnaissance, RSO is a means of "projecting power without projecting vulnerability."[60] Through RSO, the Air Force also achieves economies of scale—by utilizing a centralized global operations center, a large team employs encrypted satellite communications to conduct unmanned operations across an entire theater of war, rather than one smaller team supporting a single UAS in service for a confined area.[61] See Figure 1 for an illustration of the Remote Split Operations architecture.

[58] P. W. Singer, Wired for War: The Robotics Revolution and Conflict in the Twenty-First Century (2009), at 329 ("For a new generation, 'going to war' doesn't mean shipping off to some dank foxhole in a foreign land to dodge bullets. Instead, it is a daily commute in your Toyota Camry to sit behind a computer screen and drag a mouse. Their location doesn't limit the violence that cubicle warriors deal out, though…[Creech AFB] just outside of Las Vegas is where most of the combat action in the air force takes place today. As one drone pilot describes, 'If you want to pull the trigger and take out bad guys, you fly a Predator'").

[59] David Cenciotti, *Behind the Scenes: What It's Like Inside a Predator Drone Control Station,* TechNewsDaily, Jul. 12, 2011, *available at* http://www.technewsdaily.com/2862-behind-the-scenes-what-its-like-inside-an-unmanned-aircraft-system-station.html.

[60] Lieutenant General Dave Deptula, Deputy Chief of Staff, Intelligence/Surveillance/Reconnaissance (ISR), *Air Force Unmanned Aerial System (UAS) Flight Plan 2009-2047*, at slide 26, on file with author.

[61] *Id*., at slide 29 (The Air Force has argued that the RSO model is superior to a forward deployed line of site model since the stateside RSO operators oversee almost triple the number of combat air patrols that individual deployed teams, using more simple line of sight communications, can support).

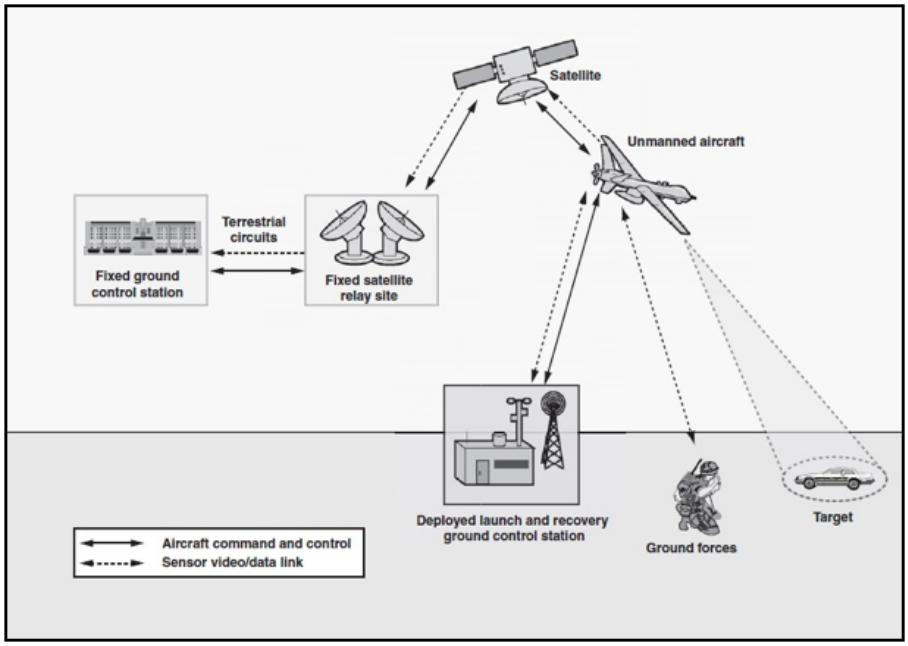


Figure 1: Remote Split Operations Architecture[62]

4. Line of Sight Operations

SUAS and Army UAS are not operated by RSO. Instead, teams deployed to the theater of war conduct these unmanned operations using sophisticated communications equipment that provides the ability to operate the UAS remotely using line-of-sight (LOS) connectivity. The complexity of the communications and data controls varies by the size, endurance, range, and capabilities of the individual aircraft. The small, hand-launched Group 1 SUAS, for example, are designed for simple ISR tasks, such as quick looks behind a building or over a hill, and require a simple remote control that fits in a backpack.[63] In comparison, Army MQ-1C Gray Eagle and MQ-5B Hunter operations are controlled from large ground control stations (GCS) with powerful communications technology.[64] See Figure 2 for an illustration of the Line of Sight Operations concept.

---

[62] U.S. Gov't Accountability Office, GAO-10-331, Unmanned Aircrafts Systems: Comprehensive Planning and a Results-Oriented Training Strategy are Needed to Support Growing Inventories, 17–18 (2010) [hereinafter GAO-10-331], *available at* http://www.gao.gov/assets/310/302236.pdf, citing GAO analysis of DoD data; Art Explosion (Images).

[63] Army Roadmap, *supra* note 45, at 22.

[64] Army Roadmap, *supra* note 45, at 10 (Despite Air Force argument that RSO was a better method of operating Group 4 and 5 UAS, the Army resisted the Air Force model of making UAS an asset of the Joint Force Commander, supporting theater needs, but rather an organic asset of the deployed unit supporting individual commanders. "The physical location of the GCS can be fixed or mobile and is dependent upon the mission and commander's requirements. All Army GCS operate via LOS and are located and controlled in the AO [area of operations] they support); Lt Col Cutting Interview, *supra* note 52 (The Gray Eagle is a Division level asset that resides in an aviation brigade. The Gray

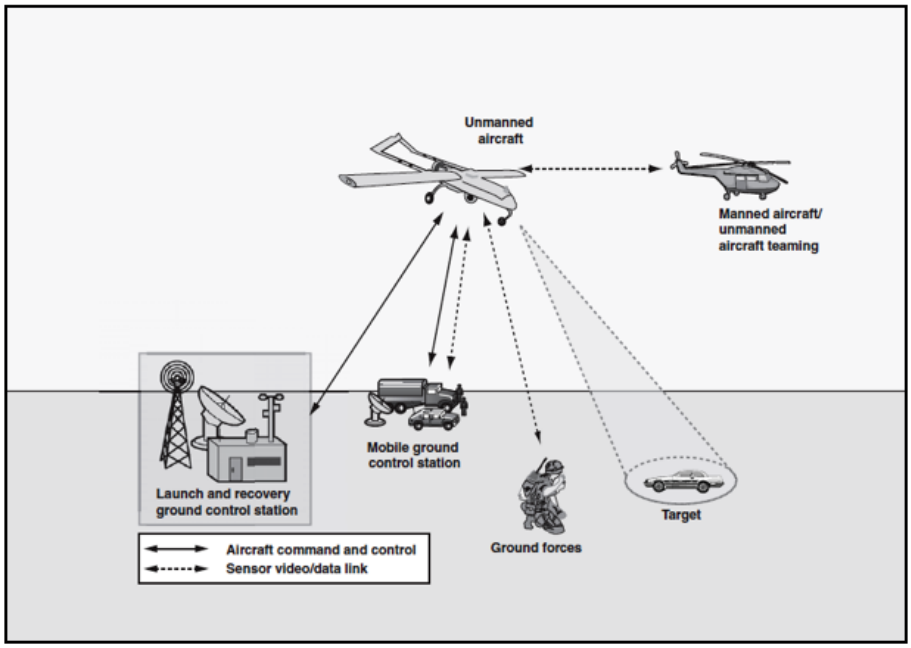


Figure 2: Line of Sight Operations Architecture[65]

A table outlining the quantities and missions of the primary DoD Unmanned Aircraft System aircraft and ground control stations is provided in Appendix B.[66]

D. Personnel Requirements

> *The only thing that is unmanned with this system is a little teeny tiny piece of fiberglass that's on the end of this very long, people-intensive spear.*[67]
> *–Lt Col Bruce Black, USAF, RPA Task Force*

It is important to recognize that the medium to large UAS aircraft make up only a single component of a very complex system. It involves U.S. based grounded flight operators, sensor operators, communications technicians, and imagery analysts,

---

Eagle mission is to support the Division and below, but "can flex up to support the JFC. With the Air Force, the MQ-1, MQ-9 are theater assets—JFACC's under JFC control, that can flex down to support subordinate commanders.")

[65] GAO 10-331, *supra* note 62, at 17, citing GAO analysis of DoD data; Art Explosion (Images).

[66] Appendix B contains a copy of J Gertler, *supra* note 42, Table 1, at 8, which is based on information provided in a briefing from Dyke Weatherington, head of the Department of Defense UAS Planning Taskforce (citing Ed Wolski, *Unmanned Aircraft Systems*, OUSD (AT&L) Unmanned Warfare, briefing, Jan. 9, 2009, p. 6. Dyke Weatherington, *Current and Future Potential for Unmanned Aircraft Systems*, OUSD (AT&L) Unmanned Warfare, briefing, Dec. 15, 2010).

[67] *The Future of Unmanned Air Power* (International Institute for Strategic Studies Conference Apr. 20, 2011) at 23:49, *available at* http://www.iiss.org/about-us/offices/washington/iiss-us-events/iiss-us-conference-the-future-of-unmanned-air-power/ (statement of Lt. Col. Bruce Black) [hereinafter *The Future of Unmanned Air Power*].

it includes fielded forces and personnel directing takeoff, landing and recovery procedures, and also includes forward deployed maintenance and logistics crews who keep the aircraft and payload (sensors, camera, radar and armament on the aircraft) mission ready. A single Combat Air Patrol (CAP) mission for an Air Force MQ-1 Predator or MQ-9 Reaper demands approximately 160 to 180 personnel to complete the 24-hour mission. The more complex Global Hawk or Navy BAMS systems can require 300 to 500 personnel; requirements are adjusted depending on the intelligence capabilities required for the mission.[68] The manning requirements for other UAS missions are likewise onerous. For instance, the Army anticipates that MQ-1C Gray Eagle Battalion organizations organic to Combat Aviation Brigades will require a minimum of 128 personnel.[69] Plans for future use of the MQ-5B Hunter include deployments of aerial reconnaissance company organizations consisting of 47 personnel.[70] For the Army's and Marines' RQ-7B Shadow aircraft, a minimum of 22 personnel are required for an aerial reconnaissance platoon, or 27 personnel to man the upgraded Shadows supporting Brigade Combat Teams.[71] These personnel do not include the other individuals located in separate organizations who are needed to address intelligence Processing, Exploitation, and Dissemination (PED) requirements.

The magnitude of these human capital requirements is obvious when one considers the explosive growth in UAS mission and future procurement plans. From the six CAPs that were being performed in 2004 to the 69 CAPs that are planned for 2013, the Air Force experienced a 1200% growth in UAS missions in less than 10 years.[72] To address the demand for more unmanned capability, the Air Force plans to use "$7.3 billion for Global Hawks and $13.1 billion for Reapers and their follow-on" between 2012 and 2020.[73] And while the Air Force has led the way for

---

[68] Cloud, *Civilian Contractors, supra* note 1 (quoting General Philip M. Breedlove, Vice Chief of Staff, Air Force, who stated that individual Global Hawk missions require a minimum of 300 people, while the Predator requires a minimum of 168 personnel per mission); Interview of Lieutenant Colonel Chris Recker, U.S. Air Force Remotely Piloted Aircraft Capabilities Division (AF/A2CU), Oct. 18, 2011 [hereinafter Lt Col Recker Interview] (stating that Global Hawk manning requirements vary between 300 to 500 personnel depending on the intelligence capabilities required for the mission); *The Future of Unmanned Air Power, supra* note 67 (Briefing materials stating that for Predator and Reaper CAPs, approximately 25% of the personnel are involved in Mission Control functions--piloting, sensor operation, mission coordination, ground systems maintenance; 45% are involved in Processing, Exploitation, & Dissemination (PED)--full motion video, signals intelligence, sensor maintenance; and 30% are involved in Launch, Recovery & Equipment (LRE)—piloting, sensor operations and aircraft maintenance. For the Global Hawk, approximately 15% is dedicated to Mission Control, 20% for LRE, and 65% for PED).

[69] Army Roadmap, *supra* note 45, at 97.

[70] *Id.* at 100.

[71] *Id.* at 99.

[72] *The Future of Unmanned Air Power, supra* note 67 (as of January 2011, the Air Force has used UAS to deliver 906 Hellfire missiles and 201 GBU-12 precision guided 500 lbs. bombs against targets).

[73] CBO Policy Options, *supra* note 35, at ix; *see also* Dep't of Def., Fiscal Year 2013 Budget Request 4–7 to 4–9 (2012) [hereinafter DoD FY2013 Budget Request], *available at* http://

much of the unmanned aircraft revolution, the other services are quickly ramping up their capabilities. The Marine Corps does not plan any additional Shadow UAS purchases as of 2011, but does intend to use $120 million to upgrade existing Shadow capabilities, and is exploring concepts for future Group 4 UAS.[74] Over the next five years, the Army intends to spend $5.9 Billion for UAS purchases and upgrades.[75] The Navy, the service which has utilized UAS technology the least in the last decade, plans significant investments. Between 2012 and 2020, the Navy intends to purchase 36 BAMS for $9.4 billion and 61 Fire Scouts for $1.0 billion.[76] The Navy also plans to acquire 100 unmanned combat aircraft systems (UCAS) by 2028 for its carrier fleets.[77]

The foregoing heavy personnel requirements, exponential mission growth, and huge demands for UAS delivered intelligence and armament have resulted in the Defense Department depending heavily on contractors to maintain medium and large category UAS, to operate aircraft and sensors on missions, and to perform intelligence analysis.[78] Moreover, contractors have proven necessary to field early versions of SUAS that have not yet been incorporated into the ground forces' standard training and operation. However, because these systems have become such a vital

---

comptroller.defense.gov/budget.html (explaining that due to recent DoD budget reductions efforts, Air Force procurement of Reaper systems will be slowed, and future-year support of the Global Hawk Block 30 variant will be cut in order to sustain U-2 continued operations and Global Hawk Block 40 procurement); Office of the Secretary of Defense, Annual Aviation Inventory and Funding Plan, Fiscal Years (FY) 2013-2042, March 2012 [hereinafter Annual Aviation], *available at* http://www.fas.org/irp/agency/dod/aviation.pdf (Projecting that the number of Global Hawk-class, Reaper, and Predator-class UAS will "grow from approximately 445 in FY 2013 to approximately 645 in FY 2022").

[74] CBO Policy Options, *supra* note 35; but *see also* Annual Aviation, *supra* note 73, at 28 ("The Marine Corps plans to replace its existing Group 3 UAS, RQ-7B Shadow systems, by fielding a multirole, Group 4 UAS in the FY2018 timeframe.").

[75] CBO Policy Options, *supra* note 35, (CBO estimates the Army will obtain 20 additional Shadows and upgrades to existing Shadows for $1.9 billion, and 107 Gray Eagles for $4.0 billion); *but see also* DoD FY2013 Budget Request, *supra* note 73 at 4-9 (indicating that Army Gray Eagle procurement plans remain relatively unchanged); Annual Aviation, *supra* note 73, at 6 (stating that "the Army will buy 164 MQ-1C Gray Eagle unmanned aircraft between FY 2013 and FY 2022 to provide persistent ISR and strike capabilities in direct support of ground forces").

[76] CBO Policy Options, *supra* note 35.

[77] Cong. Budget Office, Long Term Implications of 2012 Future Years Defense Programs (June 2011), at 28, *available at* http://www.cbo.gov/sites/default/files/cbofiles/ftpdocs/122xx/doc12264/06-30-11_fydp.pdf.; *but see also* FY2013 Budget Request, *supra* note 73, at 4-5 (stating that the Navy plans to terminate its Medium-Range Maritime Unmanned Aerial System (MRUAS) program, opting to focus on MQ-8B/8C Fire Scout upgrades).

[78] Interview with Matt Ullengren, Assistant Director, Defense Capabilities and Management Team, Government Accountability Office (Jan. 25, 2012) [hereinafter Ullengren Interview] (GAO investigations and audits of UAS procurement efforts recognized that government costs were quickly rising primarily because the DoD had not anticipated the rapid increase in the need for UAS services. This miscalculation in planning "created the need for contractors. The Predator came from a technology demonstration, not a standard program, so the military had to do *ad hoc* fielding.") (*See also* GAO-10-331, *supra* note 62)

component of U.S. power projection, we must be careful that our manning needs and high-ops tempo do not force the military to use contractors for UAS mission in violation of current law and policy on the performance of inherently governmental functions. Before proceeding with an analysis of the roles and responsibilities associated with UAS missions, the next section addresses relevant limitations placed upon contractors by federal law and policy.

III. INHERENTLY GOVERNMENTAL FUNCTION LAW AND POLICY

> *When attempting to determine what should be considered inherently governmental, the best tactic is to start with a simple question: "What does the average citizen expect the government to be doing?"*[79]
>
> *–James (Ty) Hughes*

Capitol Hill and academic circles have dedicated significant attention to the basic question of what types of government responsibilities and activities might be contracted to the private sector.[80] Central to the debate is a shared agreement in the wisdom of an inherently governmental framework—that is, a shared notion that there are certain activities that should only be performed by the government. Despite numerous pieces of legislation, regulations, and policies, our nation's leaders have yet to generate a comprehensive catalog of activities that must be performed by the government. Instead, Congress and the Executive Branch have produced substantial guidance to encourage federal agencies to identify functions that could be outsourced to the private sector. Many scholars note that this preference for outsourcing activities to the private sector gained favor during the Eisenhower administration[81] and grew in preeminence over the decades. Ultimately, this outsourcing preference resulted in the complex Office of Management and Budget ("OMB") Circular A-76 [hereinafter, OMB Circular A-76] system. Under OMB Circular A-76, agencies determine which functions are inherently governmental, which functions have to be performed by government personnel, and which functions could be competed against the private sector and potentially outsourced.[82] Based on the fact that multiple

---

[79] Interview with James (Ty) Hughes, former Deputy Gen. Counsel, Acquisitions, Office of the Sec'y of the Air Force (SAF/GCQ) (Feb. 13, 2012) [hereinafter Hughes Interview].

[80] For an extremely well written brief history of the development of "inherently governmental function" definitions, policy, and law through 2009, *see* JOHN R. LUCKEY, VALERIE BAILEY GRASSO & KATE M. MANUEL, CONG. RESEARCH SERV., R40641, INHERENTLY GOVERNMENTAL FUNCTIONS AND DEPARTMENT OF DEFENSE OPERATIONS: BACKGROUND, ISSUES, AND OPTIONS FOR CONGRESS (2009), *available at* http://www.fas.org/sgp/crs/misc/R40641.pdf.

[81] *Id*. at 5 (noting the Bureau of Budget's 1955 memorandum stated "It is the stated policy of the administration that the Federal government will not start or carry on any commercial activity to provide a service or product for its own use if such product or service can be procured from private enterprise through ordinary business channels," BOB Bulletin 55-4, Jan. 15, 1955).

[82] The preference for use of the private sector was manifested in the original 1966 publication of the Office of Management and Budget (OMB) Circular A-76, subsequently revised in 1967, 1979, 1983, 1991, 1999 and 2003, *available at* http://www.whitehouse.gov/omb/circulars/a076/a76_incl_tech_correction.html, and the Federal Activities Inventory Reform (FAIR) Act of 1998, P.L. 105-270, 112

definitions of "inherently governmental functions" have been developed over the years, and that several attempts to identify examples of such functions have been made, it appears that answering the question of what government functions are appropriate to outsource has not proven an easy task.

The remainder of this section will attempt to establish an appropriate framework by which to evaluate UAS functions. I first address initial distinctions between public and private performance of activities affiliated with governance. I then describe the late 20th Century evolution of "inherently governmental functions" law and policy. Next, I describe a framework, based upon 2011 Office of Federal Procurement Policy and military regulation and international law, for evaluating the activities involved in supporting and executing the UAS mission. In this regard, these resources divide up government responsibilities into three basic categories: (1) work the government must perform in-house because it is inherently governmental, (2) work the government should perform in house because it is closely related to inherently governmental work or for other policy reasons, and (3) work that can be contracted out to the private sector.[83]

A. Origins of the "Inherently Governmental" Classification

Western scholars generally agree that there has never existed a pure separation of the public sphere and the private sector in the United States.[84] Rather, the United States has developed as a nation through a constant interplay and exchange of government actors and the public sector. According to William J. Novak, "[t]he hallmark of American politics from this perspective is the distinctive way in which power has long been distributed along an exceedingly complex array of persons, associations, and institutions that are not easily categorized as fundamentally either public or private."[85] While the United States has adopted terminology such as

Stat. 2382 (1998) (codified as amended at 31 U.S.C. § 501 (2006)). *See also id*. at 4-5; Bernard D. Rostker, RAND, A Call to Revitalize the Engines of Government 3 (2008), *available at* http://www.rand.org/pubs/occasional_papers/2008/RAND_OP240.pdf.

[83] Luckey, *supra* note 79, at 40.

[84] William J. Novak, *Public-Private Governance: A Historical Introduction*, in Government by Contract, at 26 (Jody Freeman & Martha Minow, eds., Harvard Univ. Press 2009) (citing John R. Commons, *Legal Foundations of Capitalism* (New York: Macmillan, 1932); Harold J. Laski, *Liberty in the Modern State* (New York: Faber & Faber, 1930); Adolf A. Berle & Gardiner C. Means, *The Modern Corporation and Private Property* (New York: Harcourt, Brace & World, 1968); V.O. Key, *Politics, Parties, and Pressure Groups* (New York: Thomas Y. Crowell, 1942); Grant McConnell, *Private Power and American Democracy* (New York: Alfred A. Knopf, 1966); Joseph Schumpeter, *Capitalism, Socialism, and Democracy* (New York: Harper & Brothers, 1942); John Kenneth Galbraith, *The Affluent Society* (Boston: Houghton Mifflin, 1958); Theodore J. Lowi, *The End of Liberalism: Ideology, Policy, and the Crisis of Public Authority* (New York: Norton, 1969); Morton S. Keller, *Affairs of State: Public Life in Late Nineteenth Century America* (Cambridge MA: Harvard University Press, Belknap Press, 1977); Theda Skocpol, *Protecting Soldiers and Mothers: The Political Origins of Social Policy in the United States* (Cambridge MA: Harvard University Press, Belknap Press, 1992)).

[85] *Id*. at 27.

"privatization," "outsourcing," and "competitive sourcing" in the last several decades, partnerships between the government and the private sector have long existed. Many of the first corporations founded in the United States pursued activities that most would normally expect to be more suitable for governmental entities to oversee, for example, turnpikes, utilities, and fire protection.[86] In fact, certain functions that most would view as purely governmental, such as intelligence gathering, trace their origins to commercial enterprises.[87] Given the interplay between the public realm and private sector, some would argue that there are no functions or activities within society that are "inherently governmental."[88]

Apparently, our founding fathers also did not recognize a clear dichotomy between government and the private sector, although the framers of the *Constitution* painstakingly attempted to identify powers to be reserved for the fledgling government. As stated in a 1991 Government Accountability Office ("GAO") study, "[c]oncern about which federal agency activities are inherently governmental functions is not new. It goes back as far as the early days of the nation, as evidenced, for example, by the discussions in the *Federalist Papers* among the framers of the *Constitution* over what functions are appropriate for the federal government to exercise."[89] While the *Constitution* reserves specified powers for the Federal government, neither it nor the "authoritative commentary by Alexander Hamilton, James Madison, and John Jay" specifically discuss any categories of activities or functions that must be performed by the government and not private persons.[90]

---

[86] *Id*. at 30-31 (Novak points out that of the "335 chartered corporations formed before 1800, 219 were turnpike, bridge, and canal companies; 67 were banks and insurance companies; and 36 concerned water, fire protection, or harbor facilities. Between 1790 and 1860, 88 percent of Pennsylvania's 2,333 special charters were granted to transport, infrastructure, utility, and financial corporations (only 8 percent went to manufacturing or general business firms)" *citations omitted*).

[87] Glenn J. Voelz, *Contractors and Intelligence: The Private Sector in the Intelligence Community*, 22 Int'l J. Intelligence & Counter Intelligence 586, 588 (2009) ("Critics of government 'outsourcing' suggest that the present scope of private sector involvement in intelligence operations reflects an unprecedented shift in government policy. While the magnitude of recent commercial augmentation is certainly unprecedented, the practice itself is by no means a recent phenomenon. Not until the early twentieth century did the United States develop a permanent professional intelligence corps as part of the federal government. Prior to that time, nearly all intelligence support was acquired from the private sector, largely as an improvised affair without a formalized system of organization, doctrine, and training. In many respects, the current system marks a return to the government's earliest practices of intelligence gathering by using privately contracted nongovernmental auxiliaries hired on a short-term basis for specified tasks").

[88] Novak, *supra* note 84, at 25-27.

[89] U.S. Gen. Accounting Office, GAO/GGD-92-11, Government Contractors: Are Service Contractors Performing Inherently Governmental Functions? 2 (1991), *available at* http://archive.gao.gov/t2pbat7/145453.pdf.

[90] *Id.* at 26-27 (although James Madison commented that the power to coin money was taken from the states and provided to the Federal government in order to protect the value and regulate the metal alloy, neither he nor any of his peers expressly stated that coining money is a function that must only be performed by the government. Not finding any such declarations that certain functions were necessarily governmental, the GAO concluded that "the intent of the authors of the Constitution [regarding inherently governmental functions] is not apparent.").

B. Recent Evolution of "Inherently Governmental Functions" Law and Policy

An inherently governmental function has been described as "one that, as a matter of law and policy, must be performed by federal government employees and cannot be contracted out because it is 'intimately related to the public interest'."[91] While this definition seems simple, the question of what exactly should be regarded as inherently governmental has not been decisively resolved since the Framers first encountered the issue.[92] To date, clear lines have not been drawn, despite years of complicated efforts to reduce the size of the federal government by outsourcing work to the commercial sector.[93] Arguably, the focus of the last several decades has been less on identifying precisely what activities are inherently governmental, and more on opening doors to private enterprise.[94]

The remainder of this section will attempt to establish the framework by which to evaluate UAS functions. I first summarize attempts made through the Office of Management and Budget (OMB) Circular No. A-76, the Federal Activities Inventory Reform ("FAIR") Act of 1998, and the Federal Acquisition Regulation ("FAR") at defining an "inherently governmental function." I then discuss Office of Federal Procurement Policy (OFPP) Policy Letter 11-1, *Performance of Inherently Governmental and Critical Functions* the most recent work of the OMB to build upon, and expand the guidance of, OMB Circular A-76 and the FAIR Act. Part III will close with a brief summary of some of the key principles of OFPP Policy Letter

---

[91] Luckey, *supra* note 79, at 1.

[92] Laura G. Auletta, Eric Cho, Pamela Gouldsberry, Emile Monette, Rosanne Tarapacki, Anne Terry & Nethany Noble, *Report of the Acquisition Advisory Panel of the Office of Federal Procurement Policy and the United States Congress (Jan. 2007) [hereinafter Report of the Acquisition Advisory Panel*], at 398, *available at* https://www.acquisition.gov/comp/aap/finalaapreport.html, citing Harold H. Bruff, *Public Programs, Private Deciders: The Constitutionality of Arbitration in Federal Programs*, 67 Tex. L. Rev. 441, 458 (1989). ("The boundary of the public sector in American life has never been distinct. Our history has not produced any clear tradition allocating some functions to the government and others to the private sphere."); Hughes Interview, *supra* note 78 (stating that "any policy that proposes a one size fits all solution will always be problematic.")

[93] Steven L. Schooner, *Competitive Sourcing Policy: More Sail than Rudder?*, 13 Pub. Cont. L. J. 263, 272-78 (2004) (Professor Schooner describes the attempt at distinguishing "inherently governmental" from "commercial" as inadequate and unrealistic. At the time of his writing, policy required the Government to decide what functions were inherently governmental. Those not deemed inherently governmental, were competed against the private sector with "lowest projected cost" being the deciding factor. While both the Clinton and George W. Bush administrations championed these competitions between the government workforce and the commercial market as a mechanism for improving efficiencies and saving taxpayer funds, the primary, yet unstated, benchmark for the contemporary "competitive sourcing" policy was the reduction of government employees. Ultimately, competitive sourcing trimmed the number of government workers, but not the size of the government since the former federal workforce was essentially replaced by substitute contractors.)

[94] *Id.* at 270-71 (citing Notice of Revision, Office of Management and Budget Circular No. A-76 [hereinafter OMB Circular A-76], *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/about_omb/a76_incl_tech_correction.pdf, 68 Fed. Reg. 32,134, 32,135 (May 29, 2003), which presents both a "deference to the competitiveness of the private sector" and a irreconcilable recognition of "the value of salutary competition between the public and private sectors."

11-1, Department of Defense Instruction (DoDI) 1100.22, *Policy and Procedures for Determining Workforce Mix* and the Law of Armed Conflict (LOAC) (also known as International Humanitarian Law ("IHL")), that together present guidelines capable of assisting agencies in determining what UAS activities cannot, or should not, be contracted out. Specifically, I will build upon all of these resources to carve up the UAS mission of the U.S. Armed Forces into three basic categories: (1) work the government must perform in-house because it is inherently governmental, (2) work the government should perform in house because it is closely related to inherently governmental work or for other policy reasons, and (3) work that can be contracted out to the private sector.[95]

1. Office of Management and Budget Circular No. A-76

In 1966, OMB first published Circular No. A-76. Since that time, OMB has revised the Circular six times, the last revision and republication occurring on May 29, 2003.[96] The 2003 version of OMB Circular No. A-76 established "federal policy for the competition of commercial activities," superseding previous guidance by OMB and OFPP.[97] In support of the federal government's policy of relying on the private sector for "commercial services" in order to achieve goals of efficiency and cost savings, the A-76 Circular directed agencies to: (1) conduct inventories identifying "all activities performed by government personnel as either commercial or inherently governmental;" (2) "[p]erform inherently governmental activities with government personnel;" and (3) follow specified competition procedures to determine whether activities identified as commercial would best be provided by the private sector, in-house federal employees, or by another agency.[98] As described by Congressional Research Services, "OMB Circular A-76 has become the primary focal point for discussions of what is an inherently governmental function because it and its four attachments establish guidelines and procedures for determining whether an activity should be performed in-house with government personnel or whether it should be contracted out to the private sector."[99]

---

[95] *See* Luckey, *supra* note 79, at 40 (presenting these three tiers of consideration for potential contracting decisions).

[96] *Id*. at 5. ("The authority cited for issuing the Circular is the Budget and Accounting Act of 1921, 31 U.S.C. §§ 501-502; the Office of Federal Procurement Policy Act, 41 U.S.C. § 401 *et seq*.; and Federal Activities Inventory Reform (FAIR) Act of 1998, P.L. 105-270. OMB Circular A-76 was substantially revised in 1967, 1979, 1983, 1991, 1999, and, most recently and extensively, in May 2003. The 1999 amendment, in particular, was issued to bring the Circular into conformance with and assist in implementation of the FAIR Act.")

[97] OMB, Circular No. A-76 Revised, May 29, 2003 [hereinafter OMB Circular A-76], *available at* http://www.whitehouse.gov/omb/circulars/a076/a76_incl_tech_correction.html.

[98] *Id*.

[99] Luckey, *supra* note 79, at 5.

OMB Circular A-76 defines "commercial activity" as a "recurring service that could be performed by the private sector. This recurring service is an agency requirement that is funded and controlled through a contract, fee-for-service agreement, or performance by government personnel. Commercial activities may be found within, or throughout, organizations that perform inherently governmental activities or classified work."[100]

The A-76 Circular describes an inherently governmental activity as one "so intimately related to the public interest as to mandate performance by government personnel."[101] The activity generally is one that involves exercise of substantial discretion in applying government authority or making decisions for the government, typically binding the U.S. to action or inaction, advancing substantial interests, significantly affecting private persons, or exerting control over U.S. property or funds.[102] While the 2003 revision retained the 1999 Circular A-76 definitions, the revision created "significant loopholes by allowing for activities to be performed by contractors 'where the contractor does not have the authority to decide on a course of action, but is tasked to develop options, or implement a course of action, with agency oversight'."[103] Further, it should be noted that because Circular A-76 is drafted in support of the federal government's policy to "rely on the private sector for needed commercial services," the agency must "justify, in writing, any designation of government personnel performing inherently governmental activities."[104] This requirement for written justification of inherently governmental activities has been

---

[100] OMB Circular A-76, *supra* note 97, at Attachment D.

[101] *Id.* at Attachment A, ¶B.1.a. (The Federal Acquisition Regulation incorporates this definition of "inherently governmental" by reference, *See* 48 C.F.R. § 7.301).

[102] *Id.* (Attachment A, ¶B.1.a, in its entirety, states:

a. An inherently governmental activity is an activity that is so intimately related to the public interest as to mandate performance by government personnel. These activities require the exercise of substantial discretion in applying government authority and/or in making decisions for the government. Inherently governmental activities normally fall into two categories: the exercise of sovereign government authority or the establishment of procedures and processes related to the oversight of monetary transactions or entitlements. An inherently governmental activity involves:

(1) Binding the United States to take or not to take some action by contract, policy, regulation, authorization, order, or otherwise;

(2) Determining, protecting, and advancing economic, political, territorial, property, or other interests by military or diplomatic action, civil or criminal judicial proceedings, contract management, or otherwise;

(3) Significantly affecting the life, liberty, or property of private persons; or

(4) Exerting ultimate control over the acquisition, use, or disposition of United States property (real or personal, tangible or intangible), including establishing policies or procedures for the collection, control, or disbursement of appropriated and other federal funds).

[103] Simon Chesterman, '*We Can't Spy…If We Can't Buy!': The Privatization of Intelligence and the Limits of Outsourcing 'Inherently Governmental Functions,'* 19 Eur. J. L. Int'l 5, 1071 (2008) (citing OMB Circular A-76, at Attachment A, ¶¶ B.1.b - B.1.c).

[104] OMB Circular A-76, *supra* note 97, at ¶4 and Appendix A, ¶B.1.

interpreted as meaning that the Government has the burden to show that an activity is governmental; this has resulted in a shorthand that, unless shown otherwise, an activity is commercial and the agency must seriously consider using contractors.[105]

2. Federal Activities Inventory Reform Act of 1998

While OMB Circular No. A-76 established a process by which agencies were to compete with private entities; as policy, it did not possess the power to force agencies to investigate the potential contracting of commercial activities with the private sector. Conversely, the Federal Activities Inventory Reform (FAIR) Act of 1998[106] provided a statutory requirement that agencies compile and publicize annual lists of all commercial activities performed, and to use competitive source selection procedures if a decision is made to contract with the private sector for performance of a function.[107] Taken together, OMB Circular A-76 and the FAIR Act were seen by the Bush administration as essential mechanisms for slashing the government workforce.[108]

---

[105] Jessie Riposo, Irv Blickstein, Stephanie Young, Geoffrey McGovern & Brian McInnis, RAND, *A Methodology for Implementing the Department of Defense's Current In-Sourcing Policy*, Tech Report 944, Prepared for the United States Navy 3 (2011), *available at* http://www.rand.org/content/dam/rand/pubs/technical_reports/2011/RAND_TR944.pdf ("The polices adopted by President Clinton and President George W. Bush expanded the opportunities for the private sector in government. The burden then fell on advocates of the civil service to justify why positions should not be outsourced rather why they should").

A discussion of the A-76 Circular competitive sourcing process is beyond the scope of this paper. For a good overview of the process, *see generally* Mohab Tarek Khattab, *Revised Circular A-76: Embracing Flawed Methodologies*, 34 Pub. Cont. L. J. 469 (2005); Kate M. Manuel & Jack Maskell, Cong. Research Serv., R41810, Insourcing Functions Performed by Federal Contractors: An Overview of the Legal Issues (2011) *available at* http://www.fas.org/sgp/crs/misc/R41810.pdf; Schooner, *Competitive Sourcing Policy, supra* note 93; Kevin P. Steins & Susan L. Turley, *Uncontracting: The Move Back to Performing In-House*, 65 A.F. L. Rev. 145 (2010); Luckey, *Inherently Governmental Functions, supra*, note 78; and Paul R. Verkuil, *Outsourcing and the Duty to Govern*, in Government by Contract 310-334 (Jody Freeman & Martha Minow, eds., Harvard Univ. Press 2009).

[106] Federal Activities Inventory Reform (FAIR) Act of 1998, P.L. 105-270, 112 Stat. 2382 (codified at 31 U.S.C. § 501).

[107] 31 U.S.C. § 501, at § 2(a) & (c); *see also* Luckey, *supra* note 79, at 8 (noting there is no statutory requirement that agencies contract out a function that is determined to be commercial in nature); Schooner, *Contractor Atrocities, supra* note 4, at 556 (describing the conflicting policy that exists in the Government's determinations to employ the private sector: "Choosing between the labels "outsourcing" and "competitive sourcing" involves a significant policy decision, rather than mere semantics. In an outsourcing regime, government relies upon the private sector to perform its commercial activities. In other words, if the private sector can perform a task for the government, it should. Conversely, competitive sourcing permits existing government personnel (through the guise of a putative "most efficient organization" or MEO) to compete with the private sector to perform the same commercial activities. Under a competitive sourcing regime, the private sector only should perform commercial activities if cost savings are anticipated).

[108] Lawrence Kapp & Thomas Lum, Cong. Research Serv., RL31688, Foreign Affairs, Defense, and Trade: Key Issues for the 108th Congress, (2003), at 56 (noting that the Bush Administration's preference for the private sector is clearly recognizable in its "long-term goal of competing about 425,000 federal jobs, which represents about half of all commercial work performed by the federal

An inherently governmental function is defined statutorily in the FAIR Act as "a function so intimately related to the public interest as to require performance by Federal Government employees."[109] Similar to the broad phrasing found in the 2003 revision of OMB Circular A-76, the FAIR Act identifies inherently governmental functions as those which "require either the exercise of discretion in applying Federal Government authority or the making of value judgments in making decisions for the Federal Government."[110] The definition is supplemented by two lists of descriptions of functions that would, and would not, be included within the FAIR Act's definition of inherently governmental, as well as non-exhaustive lists of examples of included and excluded functions.[111] The FAIR Act's "inherently governmental function" definition, and agency listing requirements apply to all Federal executive branch agencies, to include the Department of Defense, with few exceptions.[112]

---

government.").

[109] 31 U.S.C. § 501, *supra* note 107, at § 5(2)(A).

[110] *Id.* (A noticeable difference is the 1998 FAIR Act's use of the phrase "exercise of discretion," as opposed to the more flexible "exercise of *substantial* discretion (emphasis added)" standard put forth later in the A-76 Circular 2003 Revision).

[111] *Id.* at § 5(2)(B); § 5(2)(C). (Both sections are provided in their entirety below)

(B) Functions included.—The term includes activities that require either the exercise of discretion in applying Federal Government authority or the making of value judgments in making decisions for the Federal Government, including judgments relating to monetary transactions and entitlements. An inherently governmental function involves, among other things, the interpretation and execution of the laws of the United States so as—

(i) to bind the United States to take or not to take some action by contract, policy, regulation, authorization, order, or otherwise;

(ii) to determine, protect, and advance United States economic, political, territorial, property, or other interests by military or diplomatic action, civil or criminal judicial proceedings, contract management, or otherwise;

(iii) to significantly affect the life, liberty, or property of private persons;

(iv) to commission, appoint, direct, or control officers or employees of the United States; or

(v) to exert ultimate control over the acquisition, use, or disposition of the property, real or personal, tangible or intangible, of the United States, including the collection, control, or disbursement of appropriated and other Federal funds.

(C) Functions excluded.—The term does not normally include—

(i) gathering information for or providing advice, opinions, recommendations, or ideas to Federal Government officials; or

(ii) any function that is primarily ministerial and internal in nature (such as building security, mail operations, operation of cafeterias, housekeeping, facilities operations and maintenance, warehouse operations, motor vehicle fleet management operations, or other routine electrical or mechanical services).

[112] Luckey, *supra* note 79, at 9-10, citing 31 U.S.C. § 501 note, at §§ 4(a)(1)-(3) and 4(b)(1)-(5), ("[T]he FAIR Act explicitly exempts from the act's requirements (1) GAO; (2) government corporations or government-controlled corporations, as defined in 5 U.S.C. § 103; (3) non-appropriated funds instrumentalities, as described in 5 U.S.C. § 2105(c); (4) certain depot-level maintenance and repair activities of the Department of Defense, as described in 10 U.S.C. § 2460; and (5) agencies with

3. Federal Acquisition Regulation

Prior to the publication of OFPP Policy Letter 11-1, there existed three "major source[s] of federal law and policy on inherently governmental functions:" the FAIR Act, OMB Circular No. A-76, and the Federal Acquisition Regulation (FAR).[113] The FAR draws from OMB Circular A-76 for its definition of the term,[114] implements the policy of OMB Circular A-76 in Section 7.5,[115] and expressly states that "[c]ontracts shall not be used for the performance of inherently governmental functions."[116] Practically mirroring the guidance provided in the FAIR Act, the FAR supplements its definition of an inherently governmental function with descriptions of functions that would, and would not, fall within the definition.[117] The FAR, however, broadened the previous policy guidance provided by the FAIR Act and OMB Circular A-76 by introducing the first lengthy lists of example functions considered as either inherently governmental activities, or not inherently governmental but possibly at risk of encroaching upon inherently governmental activities.[118]

In the aggregate, the FAIR Act, OMB Circular A-76 and the FAR provided rules for identifying inherently governmental activities to prevent improper contracting. Collectively, these three resources provide both legal and policy-based definitions of inherently governmental functions; elaborate on the meanings of definitions; provide examples of inherently governmental functions; expressly prohibit the contracting out of inherently governmental functions; define commercial activities; and introduce the possibility of contracted activities approaching inherently governmental categorization.[119] Despite these policies, regulations, and laws, their distinctions between private-public functions would benefit from greater susceptibility to simple, reliably predictable application.

---

fewer than 100 full-time employees as of the first day of the fiscal year.).

[113] *Id*. at 16.

[114] 48 C.F.R. § 7.501 (Definitions of "inherently governmental activity" and other terms applicable to this subpart are set forth at Attachment D of the Office of Management and Budget Circular No. A-76 (Revised), Performance of Commercial Activities, dated May 29, 2003 (the Circular)); 48 C.F.R. § 2.101 (defining "inherently governmental function" as "a function that is so intimately related to the public interest as to mandate performance by Government employees. This definition is a policy determination, not a legal determination.")

[115] Luckey, *supra* note 79, at 16, citing 48 C.F.R. § 7.5 ("Subpart 7.5 of the FAR is designed to provide executive branch officials with procedures for contracting out those functions that were found to be appropriate for private-sector performance under OMB Circular A-76 or other authority.").

[116] 48 C.F.R. § 7.503(a).

[117] Compare 31 U.S.C. § 501 note, at § 5(2)(B) and (C), to 48 C.F.R. § 2.201, (1)-(2) at "Inherently governmental function."

[118] 48 C.F.R. § 7.503(c)-(d). *See* Attachment A to this paper for the FAR listings.

[119] Luckey, *supra* note 79, at 27 (in Table 1, CRS produces a side-by-side concise comparison of the principle features of the treatment of inherently governmental functions by the FAIR Act, OMB Circular A-76, and the FAR).

4. Office of Federal Procurement Policy Letter 11-1

While it is unlikely that the Federal government will cure all contracting improprieties, many still regard drawing a distinct line separating those tasks that must be performed by the government from those that may be done by the private sector as a critical mission.[120] The importance many have placed on the separation of governmental activities from private activities has been heightened by recent investigations into alleged fraud, waste, and abuse committed by contractors during the last decade of war.[121] In addition to discovering billions of dollars in erroneous and unlawful fees billed to the Government, investigators identified numerous situations where contractors were inappropriately used to fill military roles, often without meaningful government oversight.[122] Such findings arguably add momentum to a pendulum many regard as swinging away from prior administrations' preferences for competitive sourcing[123] and toward the current administration's preferences for insourcing.[124]

Although Congress passed several laws during the 2000s in an attempt to curb outsourcing and protect federal civilian positions,[125] one of the strongest

[120] *Report of the Acquisition Advisory Panel, supra* note 92, at 398 ("With the growth of the multisector workforce, it has become even more important to specify which functions can and cannot legally be performed by the private sector, as well as what functions ought to be performed by federal employees").

[121] *See generally* CWC Final Report, *supra* note 2.

[122] *Id.* at 38-52. (The Commission on Wartime Contracting (CWC) focused much of its analysis on private security contracting, which had received considerable media attention due to violent incidents such as the 2007 shootings in Baghdad's Nisur Square as well as steep contract costs. In short, the CWC concluded that lack of acquisition management professionals and insufficient guidance for determining what functions were appropriate for contracting led to improper contracting decisions and inappropriate levels of reliance on contractors during the wars in Iraq and Afghanistan); consider also Hughes Interview, *supra* note 78 (stating that "There is never enough oversight of contractors. [We] never have the trained, experienced manpower to truly oversee performance. Inevitably, the contractor is placed in theater and told to do the job. They may or may not do the job. They may or may not perform as best they can.")

[123] *See generally* OMB Circular A-76, *supra*, note 93; Schooner, *Competitive Sourcing Policy, supra* note 93, at 270-71 (pointing out OMB Circular A-76 (2003) preference for the private sector).

[124] *See generally* Schooner, *Contractor Atrocities, supra* note 4, at 551-54 (stating that over the last few decades, Presidential administrations have favored a policy of outsourcing, but recent attention of contractor abuses and waste raised concerns and prompted investigations); Sandra I. Erwin, *Pentagon Insourcing Fueling Contractor Anxiety*, Nat'l Def. Magazine, Apr. 2011, *available at* http://www.nationaldefensemagazine.org/archive/2011/April/Pages/PentagonInsourcingFuelingContractorAnxiety.aspx (writing that "[b]oth Congress and the administration concluded that the [outsourcing] pendulum had swung too far."); E. Sanderson Hoe & Phillip Carter, *Feature Comment: OFPP Issues Proposed New Definition of Inherently Governmental*, 52 GC 139 (Apr. 21, 2010) (stating that 2011 OFPP Policy Letter 11-1 expresses "the Obama administration's policy preference for Government employees over contractors").

[125] *See* Steins & Turley, *Uncontracting, supra* note 105, at 148 (According to the authors, "In the 2008 National Defense Authorization Act, Congress passed legislation that almost completely reversed the presidential outsourcing efforts of the last few decades. Specifically, 10 U.S.C. § 2463

indications of outsourcing losing at least some of its preferred status materialized in a March 4, 2009 memorandum from President Obama. [126] In this memorandum to Heads of Executive Departments and Agencies, the President expressed his concern that overreliance on contractors has resulted in poor competition and waste of taxpayer dollars. For that reason, the President announced he was directing OMB to assist agencies in identifying and correcting contracts for services that have proved "wasteful, inefficient, or not otherwise likely to meet the agency's needs," and to clarify "when governmental outsourcing for services is and is not appropriate."[127] In response to the President's memorandum, Office of Federal Procurement Policy (OFPP) Letter 11-1 was published on September 12, 2011, to serve as the Executive Branch's attempt at guidelines for outsourcing "to clarify when government outsourcing of services is, and is not appropriate."[128]

The initial response to OFPP Letter 11-1 has been varied. Some recognize this guidance as a potentially helpful tool for agencies attempting to balance its workforce of federal personnel and contractors.[129] In an interview with *Government Executive* magazine, Dan Gordon, former OFPP Administrator, described the new policy letter as sensitive to the current state of the Federal budget:

> *"We need to demonstrate fiscal responsibility on both sides" of the contracting process, he said. "We don't want to dramatically increase [full-time equivalent] levels on the federal side, but in*

---

requires government agencies to consider 'using, on a regular basis, Department of Defense civilian employees to perform new functions and functions that are performed by contractors.'"); *see also* Jessie Riposo, et al., *supra* note 104, at 3 (stating that opposition to preferences for outsourcing developed in the mid-2000s in the form of governmental reviews of prior outsourcing decisions and Congressional introduction of "in-sourcing language in the National Defense Authorization Act for Fiscal Year 2006.").

[126] Steins & Turley, *Uncontracting, supra* note 105 at 156-62.

[127] Office of the President, White House Memorandum for the Heads of Executive Departments and Agencies, subject: Government Contracting, March 4, 2009, *available at* http://www.whitehouse.gov/the_press_office/Memorandum-for-the-Heads-of-Executive-Departments-and-Agencies-Subject-Government/.

[128] Publication of the Office of Federal Procurement Policy (OFPP) Policy Letter 11-01, Performance of Inherently Governmental and Critical Functions, 76 Fed. Reg. 56,227 (Sept. 12, 2011) [hereinafter OFPP Policy Letter 11-1].

[129] *See* Charles S. Clark, *OMB Announces Final Guidance on Inherently Governmental Functions*, Gov't Executive, Sep. 9, 2011, *available at* http://www.govexec.com/dailyfed/0911/090911cc1.htm. (citing Stan Soloway, president of the industry group the Professional Services Council: "We are pleased OFPP has retained flexibilities for agencies to determine what functions are considered closely associated with inherently governmental functions or are critical functions to agency missions and to provide for these functions in a way that best meets their needs and capabilities"); W. Bruce Shirk & Jessica M. Madon, *Federal "In-Sourcing": New Rules For Inherently Governmental Functions*, Gov't Contracts, Investigations & Int'l Trade Blog, June 14, 2010, *available at* http://www.governmentcontractslawblog.com/2010/06/articles/procurement-1/federal-insourcing-new-rules-for-inherently-governmental-functions/ (describing the policy letter as "a noticeable improvement over previous efforts" despite "serious shortcomings").

today's fiscal world, the solution is not massive contracting out," nor is it massive insourcing.[130]

Several individuals throughout industry, the legal community, and academia, however, have expressed concerns that the policy provides agencies with too much discretion and flexibility, has the potential to seriously hinder small businesses, and ultimately will result in poor insourcing decisions.[131]

Practically mirroring the definition provided in the FAIR Act, [132] the letter provides a single definition of "inherently governmental function;"[133] duplicates the FAIR Act's lists of activities normally included in, or excluded from, the definition of inherently governmental;[134] and includes an appendix of examples of inherently

---

[130] Clark, *OMB Announces Final Guidance, supra* note 128.

[131] *Id.* (reporting that various members of business community remarked that the letter fails to protect small business, causes confusion regarding "critical functions," and allows agencies to make insourcing decisions with little transparency or communication with incumbent businesses); Ralph C. Nash, *Contracting Out Policy: Guidance From The Office Of Federal Procurement Policy*, 24 N&CR 23 (May 2010) (Professor Nash expresses concern for future government acquisitions: "the proposed policy letter appears to give agencies considerable leeway in using contractors to perform a considerable amount of the work of the normal contracting office. While this may be necessary in some agencies because of serious staffing problems, it does not seem to be a sound long-term policy. We continue to believe that agencies should have contracting offices staffed by Government employees who can carry out the acquisition mission of the agency."); Richard Fontaine & John Nagl, Ctr. for a New Am. Sec., Contracting in Conflicts: The Path to Reform (2010), at 27, *available at* http://www.cnas.org/node/4560 (National security researchers critique the draft policy letter and suggest that a better alternative would be to focus on a "core competencies" approach, which would focus on those functions the government should develop, maintain and enforce, rather than trying to enumerate a list of specific activities for which it is impermissible to outsource. Core competencies could be outsourced, but only *in extremis*.); Daniel Goure, Ph.D., Lexington Institute, *New OMB Policy On Critical Functions Opens The Door To More Insourcing,* Early Warning Blog, Sep. 14, 2011, *available at* http://www.lexingtoninstitute.org/new-omb-policy-on-critical-functions-opens-the-door-to-more-insourcing?a=1&c=1171 ("Although the OMB policy correctly leaves the identification of critical and closely associated functions up to the agencies, it does nothing to place restraints on the natural tendency of bureaucrats to a) build their own empires through insourcing or b) just cover their behinds when in doubt."); E. Sanderson Hoe & Justin M. Ganderson, OFPP *Issues Final Policy Letter Defining "Inherently Governmental Functions*," Sep. 20, 2011, *available at* www.mckennalong.com (Government contract attorneys criticize the letter for failing to provide a clear definition of "closely associated functions" or "critical functions" the letter gives several examples of closely associated functions, but only two examples of critical functions).

[132] L. Elaine Halchin, Kate M. Manuel, Shawn Reese & Moshe Schwartz, Cong. Research Serv., R41209, Inherently Governmental Functions and Other Work Reserved for Performance by Federal Government Employees: Obama Admin's Proposed Policy Letter (2010) ("In keeping with the requirements of Section 321 of the Duncan Hunter National Defense Authorization Act for FY2009 (P.L. 110-417), which tasked OMB with developing a "single consistent definition" of "inherently governmental function," the proposed policy letter adopts the definition of the Federal Activities Inventory Reform (FAIR) Act.")

[133] OFPP Policy Letter 11-1, *supra* note 127, at §3 (adopting the definition provided in 31 U.S.C. § 501 note, *supra* note 106, at § 5(2)(A)).

[134] *Id.* at §3(a)-(b) (adopting the functions included within, and excluded from, the definition of inherently governmental, as provided in 31 U.S.C. § 501 note, *supra* note 106, at §§ 5(2)(B)-(C)).

governmental functions:[135] The following inherently governmental functions relevant to the UAS operational mission are listed as follows in the Policy Letter 11-1 Appendix:

> *3. The command of military forces, especially the leadership of military personnel who are performing a combat, combat support or combat service support role.*
>
> *4. Combat.*
>
> *5. Security provided under any of the circumstances set out below. This provision should not be interpreted to preclude contractors taking action in self-defense or defense of others against the imminent threat of death or serious injury.*
>
> > *(a) Security operations performed in direct support of combat as part of a larger integrated armed force.*
> >
> > *(b) Security operations performed in environments where, in the judgment of the responsible Federal official, there is significant potential for the security operations to evolve into combat. Where the U.S. military is present, the judgment of the military commander should be sought regarding the potential for the operations to evolve into combat.*
> >
> > *(c) Security that entails augmenting or reinforcing others (whether private security contractors, civilians, or military units) that have become engaged in combat.*
> >
> > . . .
>
> *11. The direction and control of Federal employees.*
>
> *12. The direction and control of intelligence and counter-intelligence operations.*[136]

---

[135] *Id.* at Appendix A. "Examples of inherently governmental functions."

[136] *Id.* (OFPP Policy Letter 11-1 adopts the FAR 7.503 list of inherently governmental functions, but adds the separate functions of "combat" and "security" that meet the criteria set forth in 5(a)-(c). As explained in the Responses to Commentary regarding the examples provided for inherently governmental functions, "Based on public comment and additional deliberations, OFPP has added to the list of inherently governmental functions: (i) All combat and (ii) security operations in certain situations connected with combat or potential combat. OFPP concluded these were clear examples of functions so intimately related to public interest as to require performance by Federal Government employees; hence, the addition of these activities to the list of inherently governmental functions would contribute to clarifying the line between what work must be reserved for Federal employees and what work may be performed by contractors.").

According to the letter's guidelines, all functions should be assessed according to two separate tests based upon (1) the *nature of the function* and (2) the *degree of discretion exercised by the function*.[137] According to the first test, the exercise of the sovereign powers of the United States is inherently governmental, regardless of the level of discretion exercised. Examples presented include "in an inter-governmental forum or body, arresting a person, and sentencing a person convicted of a crime to prison."[138]

Under the second test, *exercise of discretion*, a function is regarded as inherently governmental (1) where the exercise of discretion "commits the government to a course of action where two or more alternative courses of action exist and decision making is not already limited," (2) where the function has the "authority to decide the course of action" and agency official would not possess "the ability to override the contractor's action," or (3) "where the contractor's involvement is or would be so extensive, or the contractor's work product so close to a final agency product, as to effectively preempt the Federal officials' decision-making process, discretion or authority."[139]

The letter also provides guidance for agency evaluation of work "closely associated" with inherently governmental functions, explaining that agencies must provide special management attention to contractor activities where there is a "risk that performance may impinge on Federal officials' performance of an inherently governmental function."[140] An illustrative appendix of examples of closely associated functions that agencies should carefully assess before outsourcing is provided.[141] Regarding the evaluation of security services, the commentary explains that such "situations should be evaluated on a case-by-case basis to determine what security functions and activities are inherently governmental and what can be performed by contractors with appropriate management and oversight."[142]

The letter expands on previous policies by requiring agencies to identify "critical functions," a new category referencing functions that are core to an agency's

---

[137] *Id.* at 5-1(a)(1).

[138] *Id.* at 5-1(a)(1)(i).

[139] *Id.* at 5-1(a)(1)(ii)(A)-(C).

[140] *Id.* at 5-1(a)(1)(ii)(C)(2); *see also* CWC Final Report, *supra* note 2, at 43 (the CWC endorsed the proposed Policy Letter that was published for commentary in Federal Register, 75:61, March 31, 2010, 16188-16197, stating that OFPP "has taken a helpful step in discussing risk factors as part of the considerations to be weighed in making decisions on contracting. The OFPP's proposed policy letter on 'Work Reserved for Performance by Federal Government Employees' responds to congressional direction that tasked OMB with developing a 'single consistent definition' of 'inherently governmental function'.").

[141] *Id.*, at Appendix B, "Examples Of Functions Closely Associated With The Performance Of Inherently Governmental Functions."

[142] *Id.* at Responses to Comment 2.

mission over which sufficient internal capability must be maintained. Guidelines for identifying inherently critical functions are provided as follows:

> *The criticality of the function depends on the mission and operations, which will differ between agencies and within agencies over time. In making that determination, the officials shall consider the importance that a function holds for the agency and its mission and operations. The more important the function, the more important that the agency have internal capability to maintain control of its mission and operations."*[143]

Also, OFPP describes actions agencies should take to prevent erroneous contracting of work that should only be done by government personnel, and describes precautions agencies must take with contractors performing activities closely associated with inherently governmental functions.

5. Department of Defense Workforce Planning

Last revised on April 12, 2010, DoDI 1100.22, *Policy and Procedures for Determining Workforce Mix*, provides consolidated direction from Circular No. A-76, the United States Code, and the Federal Acquisition Regulation (FAR). The DoDI is designed to help Human Resources officers identify activities as (1) inherently governmental, (2) commercial but not subject to contracting, or (3) commercial and appropriate for outsourcing.[144] In determining the appropriate mix of military, federal civilian, and contractor manpower, the DoD affords highest prioritization to successful mission execution, stating that "risk mitigation shall take precedence over cost savings when necessary to maintain appropriate control of Government operations and missions…[or] core capabilities and readiness."[145]

DoDI 1100.22's basic definition of inherently governmental activities effectively restates with slight modification the definition found in Circular No. A-76.[146] The Instruction, however, also introduces a workforce mix decision process that relies on sixteen criteria that human resources officers and manpower analysts are instructed to use. These criteria are designed to determine which functions are inherently governmental, and which might be considered commercial

---

[143] *Id.* at 5-1(b).

[144] Dep't of Def., Instruction No. 1100.22, Policy and Procedures for Determining Workforce Mix ¶ 1 (2010) [hereinafter DoDI 1100.22], at ¶1.d., ¶1.e., and ¶4.d.

[145] *Id.* at ¶4.a.

[146] *Id.* at Enclosure 3, ¶1.b. ("In general, a function is IG [Inherently Governmental] if it is so intimately related to the public interest as to require performance by Federal Government personnel. IG functions shall include, among other things, activities that require either the exercise of substantial discretion when applying Federal Government authority, or value judgments when making decisions for the Federal Government, including judgments relating to monetary transactions and entitlements.")

and appropriate for private sector performance.[147] Additionally, functions deemed not inherently governmental and appropriate for private sector performance may become inherently governmental "because of the way they are performed or the circumstances under which they are performed."[148] The Instruction prohibits the contracting of any functions that are identified as inherently governmental by the manpower mix criteria, or that "restrict or put at risk the discretionary authority, decision-making responsibility, or accountability of Defense officials."[149] Both the FAR and OFPP Policy Letter 11-1 identify the command and performance of combat operations, and the direction and control of intelligence and counter-intelligence operations as inherently governmental functions.[150] The Policy Letter added combat and security functions under certain circumstances to its list of inherently governmental function.[151] Neither resource, however, defines combat or intelligence operations. In response, Department of Defense guidance and several principles of the Laws of Armed Conflict (LOAC) add substance to the working definitions of the foregoing discussion within the context of the policy, regulations, and laws governing inherently governmental functions.

6. Understanding "Combat" and "Direction and Control of Intelligence"

(a) *Department of Defense Guidance*

While "combat" is not specifically defined in Joint Publication 1-02 (JP 1-02), *Department of Defense Dictionary of Military and Associated Terms*,[152] a definition that would apply to UAS missions can be constructed based on related definitions and descriptions provided in the dictionary and other sources. Building upon existing doctrine regarding joint military operations,[153] JP 1-02 defines "combat power" as "[t]he total means of destructive and/or disruptive force which a military unit/formation can apply against the opponent at a given time."[154] This fairly basic definition is broadened through DoD's treatment of the concept of "combat

[147] *Id.* at Enclosure 3, ¶1.a; *see also* CWC Final Report, *supra* note 2, at 45-46 (Although the CWC authors applauded DoDI 1100.22's manpower mix decision procedures and its recognition that facts and circumstances may convert commercial activities into inherently governmental functions, they noted that the Instruction is not drafted for contingency operations and is not a regulation that is mandatory outside of the DoD.)

[148] *Id.* at ¶2.b., citing FAR 7.503(d) and 10 U.S.C. §2383.

[149] *Id.* at Enclosure 3, ¶1.b.

[150] 48 C.F.R. § 7.503(c)(3) and (c)(8); OFPP Policy Letter 11-1, *supra* note 128, at Appendix A "Examples of inherently governmental functions," (3) and (12).

[151] OFPP Policy Letter 11-1, *supra* note 127, at Appendix A. "Examples of inherently governmental functions," (4) and (5).

[152] JP 1-02, *supra* note 8 (The dictionary's purpose is to assist communications within and between the Services, other agencies, and U.S. allies by supplementing existing dictionaries and standardizing military terminology).

[153] Department of Defense, Joint Publication 3-0, Joint Operations, last revised Aug. 11, 2011, *available at* http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf.

[154] JP 1-02, *supra* note 8, at 59.

operations," presented in DoDI 1100.22, which describes when the need for combat power arises, general authority, and the actions involved.[155] The Instruction designates combat as inherently governmental and exclusively restricted to performance by the military.[156] Further, the Instruction states that manpower requirements shall be designated as inherently governmental combat "if the planned use of destructive combat capabilities is part of the mission assigned to this manpower."[157]

> *This includes manpower located both inside and outside a theater of operations if the personnel operate a weapon system against an enemy or hostile force (e.g., bomber crews, inter-continental ballistic missile crews, and* **unmanned aerial vehicle operators***). This does not include technical advice on the operation of weapon systems or other support of a non-discretionary nature performed in direct support of combat operations.*[158]

As previously mentioned, the "direction and control of intelligence" is designated as inherently governmental. JP 1-02 defines intelligence as "[t]he product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity which results in the product and to the organizations engaged in such activity."[159] The dictionary also recognizes several types of intelligence products and activities related to military operations, such as "combat intelligence,"[160] "combat surveillance,"[161] "combat identification,"[162]

---

[155] DODI 1100.22, *supra* note 144, at Enclosure 4, ¶1.c, ("[w]hen armed fighting or use of force is deemed necessary for national defense, the Department of Defense may authorize deliberate destructive and/or disruptive action against the armed forces or other military objectives of another sovereign government or against other armed actors on behalf of the United States. This entails the authority to plan, prepare, and execute operations to actively seek out, close with, and destroy a hostile force or other military objective by means of, among other things, the employment of firepower and other destructive and disruptive capabilities.")

[156] *Id.* at Enclosure 4, ¶1.c.(1). (DoDI 1100.22 effectively adopts OMB Circular A-76 *supra* note 94, and FAR parts 2 and 7.5, *supra* note 114, explanations of why combat is inherently governmental, namely that combat involves discretionary decisions regarding the exercise of sovereign power that can "significantly affect the life, liberty, or property of private persons or international relations."

[157] *Id.* at Enclosure 4, ¶1.c.(2). DoDI 1100.22 also describes certain security operations as inherently governmental if performed "in direct support of combat" or "performed in environments where there is such a high likelihood of hostile fire, bombings, or biological or chemical attacks by groups using sophisticated weapons and devices that, in the judgment of the military commander, the situation could evolve into combat." (*see* Enclosure 4, ¶1.d.(1)).

[158] *Id.* (emphasis added.)

[159] *Id.* at 168.

[160] JP 1-02*, supra* note 8, at 59 ("That knowledge of the enemy, weather, and geographical features required by a commander in the planning and conduct of combat operations.").

[161] *Id.* at 60 ("A continuous, all-weather, day-and-night, systematic watch over the battle area in order to provide timely information for tactical combat operations.").

[162] *Id.* at 58 ("The process of attaining an accurate characterization of detected objects in the

"combat information,"[163] "strategic intelligence,"[164] "tactical intelligence,"[165] "processing and exploitation,"[166] and "dissemination and integration."[167] According to DoDI 1100.22, not only would the direction and control of such intelligence activities be considered inherently governmental, but likewise the performance of "intelligence or counterintelligence activities/operations that require the exercise of substantial discretion in applying government authority and/or making decisions for the government."[168]

(b) *The Law of Armed Conflict*

While DoD publications provide definitions and explanations of "combat" and "intelligence" that help distinguish activities considered inherently governmental, additional guidance is provided by internationally accepted authority, such as the Law of Armed Conflict (LOAC), often referred to as International Humanitarian Law (IHL).[169] The four Geneva Conventions, which became effective in 1949, currently serve as the foundation of contemporary LOAC.[170] These Conventions prescribe

operational environment sufficient to support an engagement decision.").

[163] *Id*. at 59 ("Unevaluated data, gathered by or provided directly to the tactical commander which, due to its highly perishable nature or the criticality of the situation, cannot be processed into tactical intelligence in time to satisfy the user's tactical intelligence requirements.").

[164] *Id.* at 324 ("Intelligence required for the formation of policy and military plans at national and international levels. Strategic intelligence and tactical intelligence differ primarily in level of application, but may also vary in terms of scope and detail.").

[165] *Id.* at 335 ("Intelligence required for the planning and conduct of tactical operations.").

[166] *Id.* at 274 ("In intelligence usage, the conversion of collected information into forms suitable to the production of intelligence.").

[167] *Id.* at 103 ("In intelligence usage, the delivery of intelligence to users in a suitable form and the application of the intelligence to appropriate missions, tasks, and functions.").

[168] DoDI 1100.22, *supra* note 144, at Enclosure 4, ¶5.g.(7) (DoDI 1100.22 effectively adopting OMB Circular A-76, *supra* note 45, and FAR parts 2 and 7.5, *supra* note 57, stating that intelligence activities are considered inherently governmental when the activity is "military-unique.") According to DoDI 1100.22, Enclosure 4, ¶1.b.(1), "[t]he unique nature of the military establishment and its role in defense of the Nation has been recognized by the Supreme Court—i.e., the differences between the military and civilian communities result from the fact that it is the primary business of armies and navies to fight or be ready to fight wars should the occasion arise."

[169] Won Kidane, *The Status of Private Military Contractors Under International Humanitarian Law*, 38 Denv. J. Int'l L. & Pol'y 361 (2010) (describing the term "International Humanitarian Law" as a recently coined phrase not contained within the original 1949 Geneva Conventions, citing Christopher J. Greenwood, *Historical Development and Legal Basis*, in The Handbook of International Humanitarian Law 1-15 (Dieter Fleck ed., 2nd ed. 2008) [hereinafter Fleck]. "International Humanitarian Law comprises all those rules of international law which are designed to regulate the treatment of the individual - civilian or military, wounded or active - in international armed conflicts." *Id.* at 11).

[170] Rebecca R. Vernon, *Battlefield Contractors: Facing the Tough Issues*, 33 Pub. Cont. L.J. 369, 403 (2004) (stating that all parties to the four Geneva Conventions of 1949, *see infra* notes 169-74, must follow their terms, and that "the international community views most of the concepts as customary international law).

rules for the treatment of the wounded and sick in armed conflict,[171] the protection of armed forces at sea,[172] the treatment of prisoners of war,[173] and the protection of civilians during armed conflict.[174] The protections afforded civilians and members of armed forces by the Geneva Conventions were expanded through the 1977 release of two supplemental protocols: the first addressing international conflicts[175] and the second, noninternational conflicts.[176] Because the United States is not a party to the First Protocol it is not required to adhere to its provisions; however, some of Protocol's provisions are recognized as customary international law, to which the United States complies.[177]

Much scholarship has been dedicated to the history and development of LOAC and the international laws of war, as well as the expansion of humanitarian concerns for civilians during wartime, permissible weaponry, and the treatment of captured adversaries. Additionally, LOAC specifically provides useful guidance on the proper classification of contractors in relation to warfare, as well as the types of activities contractors are permitted to perform in support of military operations.[178] In particular, the following sections discuss the pertinent LOAC considerations for UAS use in the contexts of lawful combatants, civilians, and unlawful combatants. These discussions include the commonly recognized categories of individuals during times of war, and the general principle of "direct participation in hostilities."

---

[171] Geneva Convention for the Amelioration of the Condition of Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31 (entered into force Oct. 21, 1950) [hereinafter Geneva Convention I].

[172] Geneva Convention for the Amelioration of the Condition of Wounded and Sick and Shipwrecked Members of Armed Forces at Sea, Aug. 12, 1949, 6 U.S.T. 3316 (entered into force Oct. 21, 1950) [hereinafter Geneva Convention II].

[173] Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 (entered into force Oct. 21, 1950) [hereinafter Geneva Convention III].

[174] Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287 (entered into force Oct. 21, 1950) [hereinafter Geneva Convention IV].

[175] Protocol Additional to the Geneva Conventions of Aug. 12, 1949, and Relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I].

[176] Protocol Additional to the Geneva Conventions of Aug. 12, 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 609 [hereinafter Additional Protocol II].

[177] Vernon, *supra note* 170 (citing *The United States Position on the Relation of Customary International Law to the 1977 Protocol Additional to the 1949 Geneva Convention*, 2 AM. U.J. INT'L L. & POL'Y 419 (1987)).

[178] While these subjects are beyond the scope of this paper, for an overview of these matters *see generally* Fleck, *supra note* 169; Adam Roberts & Richard Guelff, Documents on the Laws of War, (3rd ed. 2004); International Humanitarian Law: Origins (John Carey et al., eds., 2003); Yoram Dinstein, The Conduct of Hostilities under the Law of International Armed Conflict (2004).

Lawful Combatants

Most scholars agree that the Geneva Conventions recognize only two categories of individuals during international armed conflict: lawful combatants and civilians.[179] Both the United States and Israel, however, take the position that there are three categories: "lawful combatants, unlawful combatants, and civilians."[180] With few exceptions, lawful combatants include only those members of organized armed forces.[181] In order to be considered a member of an armed force, one must comply with four criteria: (1) be commanded by a person responsible for his subordinates; (2) have a fixed distinctive emblem recognizable at a distance; (3) carry arms openly; and (4) conduct operations in accordance with the laws and customs of war.[182] If captured, lawful combatants are considered prisoners of war, and are entitled to the protections of the Geneva Conventions, and supplemental Protocols.[183] As lawful combatants, military members can be targets of attack by opposing armed forces, but also may lawfully target opposing armed forces without relinquishing combatant immunity from punishment for injury and/or death caused to enemy forces, weapons, or property.[184]

Civilians

Civilians, or noncombatants, are described under LOAC as individuals not participating in international armed conflict, and who enjoy immunity from attack

---

[179] Curtis A. Bradley, *The United States, Israel & Unlawful Combatants*, 12 Green Bag 397, 398 (2009).

[180] *Id*. at 399.

[181] Protocol I describes "armed forces" as follows: "organized armed forces, groups and units which are under a command responsible to that Party for the conduct of its subordinates." Protocol I, *supra* note 175, art. 43(2).

[182] Michael E. Guillory, *Civilianizing the Force: Is the United States Crossing the Rubicon*, 51 A.F. L. Rev. 111, 114 (2001) (citing 1907 Hague Convention No. IV Respecting the Laws and Customs of War on Land, Oct. 18 1907, art. 1, regulations, 36 Stat. 2277, 205 Consol. T.S. 277 [hereinafter Hague IV]; Geneva Convention I, *supra* note 171, art. 13(2); Geneva Convention II, *supra* note 172, art. 13(2); Geneva Convention III, *supra* note 173, art. 4A(2); Additional Protocol I, *supra* note 175); Guillory notes that the language describing the four criteria was altered slightly in Protocol I in an "attempt to relax the rules about wearing a distinctive uniform and carrying arms openly."

[183] Heaton, *Civilians at War, supra* note 20, at 169 (according to Heaton, "Because POWs are, in most circumstances, simply combatants who fall into the hands of the enemy, the definition of who is entitled to POW status is all but synonymous with who is a combatant," citing Knut Ipsen, *Combatants and Non-Combatants*, in Fleck, *supra* note 169, at 81).

[184] Geoffrey S. Corn, *Thinking the Unthinkable: Has the Time Come to Offer Combatant Immunity to Non-State Actors?*, 22 Stan. L. & Pol'y Rev. 253, 265 (2011), citing Geneva Convention III, *supra* note 173, art. 13 (Corn describes the immunity as a sweeping protection afforded armed forces: "Combatant immunity exacts an obvious toll from the ability to punish individuals who act to harm the state. Indeed, the immunity extended to a captured enemy soldier who qualifies for POW status deprives the detaining power of punishing the soldier not only for fighting against the state, but even for killing members of the detaining powers armed forces.").

"unless and for such time as they take a direct part in hostilities."[185] Although granted immunity from attack—that is, designated as not targetable under the LOAC principle of distinction—civilians located near the battlespace are certainly at risk of injury, death, or even capture.[186] This has long been recognized as a risk for civilians accompanying the armed forces and on site of lawful targets, such as forward operating bases in a theater of war.[187]

Unlawful Combatants

The term "unlawful combatant" originated in the 1942 United States Supreme Court case, *Ex Parte Quirin*, and has been used by the United States since that decision as a label for those civilians who act in a manner that would extinguish their protected status.[188] "The citizen must be a citizen and not a soldier . . . war law has a short shrift for the non-combatant who violates its principles by taking up arms."[189] To retain the immunities and protections afforded civilian status, an individual is required to stay out of the battle.[190] Any civilian who directly participates in hostilities is considered an illegal belligerent (or unlawful combatant to use U.S. terminology), loses all protection from lawful attack, and may be subjected to punishment for his or her actions.[191] If prisoner of war (POW) status and combatant immunity is lost, a civilian who is captured by opposing forces faces

---

[185] Protocol I, *supra* note 175, art 51.3.

[186] Eric Christensen, *The Dilemma of Direct Participation in Hostilities,* 19 J. Transnat'l L. & Pol'y 281, 285 (2010) ("The 'Basic Rule' of LOAC is that combatants and military objectives will be distinguished from civilians and civilian objects, with force directed towards the former and away from the latter."(citing Additional Protocol I, *supra* note 175, art. 48; Additional Protocol II, *supra* note 176, arts. 13-14) "This principle, known as distinction, is at the heart of DPH [Direct Participation in Hostilities]." *Id*. citing Helen Duffy, The "War on Terror" and the Framework of International Law 228-29 (2005)).

[187] Civilians in war are always at risk of being lawfully killed or injured as "collateral damage" or taken as prisoners by opposing forces. For general discussions of the risks civilians face in the theater of war, *see* Steven J. Zamparelli, *Contractors on the Battlefield: What Have We Signed Up For?*, A. F. J. of Logistics, Vol. 23, No. 3, Fall 1999, at 11–12; Lisa L. Turner & Lynn G. Norton, *Civilians at the Tip of the Spear*, 51 A.F. L. Rev. 1, 26 (2001); Guillory, *Civilianizing the Force, supra* note 182, at 115; Karen L. Douglas, *Contractors Accompanying the Force: Empowering Commanders with Emergency Change Authority*, 55 A.F. L Rev. 127, 134-35 (2004); Vernon, *supra note* 170, at 413; Geoffrey S. Corn, *Unarmed but How Dangerous? Civilian Augmentees, the Law of Armed Conflict, and the Search for a More Effective Test for Permissible Civilian Battlefield Functions*, 2 J. Nat'l Sec. L. & Pol'y 257, 258-59 (2008).

[188] Christensen, *supra* note 186, at 286 (stating that this particular categorization is not recognized by international treaty and has been subject to a significant amount of criticism, particularly in regard to its application to detainees held by the United States at Guantanamo Bay, Cuba).

[189] Douglas, *supra* note 187, at 134 (citing W. Hays Parks, *Air War and the Law of War*, 32 A.F. L. Rev. 1, 75, 118 (1990), quoting James Maloney Spaight, War Rights on Land 38 (London, 1911)).

[190] Turner & Norton, *supra* note 187, at 27.

[191] *Id.* at 25, citing Hague IV, *supra* note 182, art.3; Geneva Convention III, *supra* note 173, arts. 36, 37; Additional Protocol I, *supra* note 175, arts. 43, 44.

the possibility of criminal prosecution.[192] Given these risks—in addition to the basic risks of armed conflict—civilians accompanying the armed forces understandably would want to avoid direct participation in hostilities. But as many experts note, this is yet another important area of law that is not well defined.[193]

C. Moving Forward: A Synthesized Approach to Analyzing Government Functions

Several key principles are identified above in OFPP Policy Letter 11-1, DoDI 1100.22 and the Laws of Armed Conflict (LOAC). These key principles form important benchmarks for analyzing the use of contractors for UAS missions. One important benchmark is these authorities identify certain activities that are clearly governmental and should never be performed by civilian contractors. Each also recognizes that certain functions, while not inherently governmental, could become inherently governmental because they are closely associated with core government activities or impinge upon the discretion of government authorities. Further, these authorities recognize the need to guard against the loss of core capabilities, and overreliance on civilian contractors to perform critical functions. These key principles will be applied throughout the Part IV analysis of contractor involvement with the UAS mission.

---

[192] *See id*. at 32, 69-70 (describing unlawful combatants' loss of POW status and the possibility of prosecution for war crimes by the International Criminal Court (ICC) or "under the law of the Detaining Power"); Vernon, *supra note* 170, at 417 ("Parties may prosecute as war criminals those contractor employees taking a direct part in hostilities. Acts of hostility committed by private individuals are punishable as war crimes, not because those actions are contrary to the law of armed conflict, but because it is unlawful for private individuals to wage war"); Michael N. Schmitt, *Humanitarian Law and Direct Participation in Hostilities by Private Contractors or Civilian Employees,* 5 Chi. J. Int'l L. 511, 519-21 (2005) (stating that civilians who directly participate in hostilities may be targeted and could be punished/prosecuted for their actions; unprivileged belligerents lose all combatant immunity); Stephen M. Blizzard, *Contractors on the Battlefield: How Do We Keep From Crossing the Line?*, A. F. J. of Logistics, Spring 2004, at 11 (describing the 2002 Rome Statute that created the International Criminal Court (ICC) ability to prosecute war crimes); Rock, *supra* note 20, at 62-63 (stating that the United States decided not to ratify the ICC Rome Convention in part because of fear of possible contractor prosecutions).

[193] Corn, *Unarmed, supra* note 187, at 258-59 (quoting a 2005 electronic mail message from W. Hays Parks, Office of the General Counsel, Department of Defense, to Colonel Michael Meier, Chairman of the Joint Chiefs of Staff Office of the Legal Advisor (May 4, 2005): "As civilians accompanying the armed forces in the field, in accordance with Article 4A(4) and (5), GPW [Geneva Convention III], contractors are entitled to prisoner of war status if captured. Contractors in an active theater of operations during armed conflict are at risk of incidental injury as a result of enemy operations. A contractor may be subject to intentional attack for such time as he or she takes a direct part in hostilities. A contractor who takes a direct part in hostilities (a phrase as yet undefined, and often situational) remains entitled to prisoner of war status, but may be subject to prosecution if his or her actions include acts of perfidy; Article 85, GPW.")

IV. ANALYSIS OF CURRENT UAS FUNCTIONS AND CONTRACTOR ROLES

We're simply not going to go to war without contractors.[194]
–Ashton B. Carter

A. Contractors and Contingency Operations

Commentators have long recognized the important, and pervasive roles, civilian contractors have played in the wars in Iraq and Afghanistan.[195] Much has been written on the contributions contractors in the theaters of war have made toward installation and personnel security, weapons systems maintenance, intelligence collection and analysis, interpretation, interrogation, and various forms of logistical support.[196] In fact, without the assistance of private contracting firms, the U.S. armed forces simply could not have conducted sustained military operations in Afghanistan, Iraq and other hot spots around the world for the last ten years. With massive active duty force reductions occurring between 1989 and 1999, and the development and fielding of incredibly complex technical weapons, the U.S. military did not possess the manning or technical specializations necessary to conduct modern operations unassisted.[197] Reliance on contractors grew so rapidly that by 2010, the number of

---

[194] CWC Final Report, *supra* note 2, at 18 (citing Dr. Ashton B. Carter, Under Secretary of Defense for Acquisition, Technology, and Logistics, Commission Hearing, Mar. 28, 2011, transcript, 39).

[195] For a concise discussion of the widespread privatization of numerous federal activities and formerly military functions, *see* Steven L. Schooner & Daniel S. Greenspahn, *Too Dependent on Contractors? Minimum Standards for Responsible Governance*, J. of Cont. Mgmt. 9 (Summer 2008) (citing Mark L. Goldstein, *America's Hollow Government: How Washington Has Failed the People*, Ch. 6 (Irwin Pub. 1992); T. Christian Miller, *Private Contractors Outnumber U.S. Troops in Iraq*, L.A. Times, July 4, 2007; Paul C. Light, *Outsourcing and the True Size of Government*, 33 Pub. Cont. L. J. 311, 311-20 (2004); Martha Minow, *Outsourcing Power: How Privatizing Military Efforts Challenges Accountability, Professionalism, and Democracy*, 46 B.C. L. Rev. 989 (2005); Cong. Budget Office, Logistics Support for Deployed Military Forces, 23-25, Oct. 2005; Albert A. Robbert, Susan M. Gates, & Marc N. Elliott, RAND, Outsourcing of DOD Commercial Activities: Impacts on Civil Service Employees, (1997); Privatization: The Provision of Public Services by the Private Sector (Roger L. Kemp ed., 2007); Martha Minow, Partners, Not Rivals: Privatization and the Public Good (2003); E. S. Savas, Privatization and Public-Private Partnerships (2000); Laura A. Dickinson, *Public Law Values in a Privatized World*, 31 Yale J. Int'l L. 383, 401–22 (2006); Jody Freeman, *Extending Public Law Norms Through Privatization*, 116 Harv. L. Rev. 1285 (2003).

[196] *See generally* CWC Final Report, *supra* note 2; Dickinson, Outsourcing War & Peace, *supra* note 4; Fontaine & Nagl, Contracting in Conflicts, *supra* note 131, at 5; Heaton, *Civilians at War, supra* note 20, at 155; Michael N. Schmitt, *War, International Law, and Sovereignty: Reevaluating the Rules of the Game in a New Century: Humanitarian Law and Direct Participation in Hostilities by Private Contractors or Civilian Employees*, 5 Chi. J. Int'l L. 511, 511-14 (2005); Schooner, *Contractor Atrocities, supra* note 4, at 554; Schwartz & Swain, *supra* note 2; Turner & Norton, *supra* note 187, at 22-23; Vernon, *supra* note 170 at 369.

[197] Guillory, *supra* note 182, at 111 ("[F]rom 1989 to 1999 the active duty force size was reduced from 2,174,200 to 1,385,700. This tradeoff has not come without consequences. The drawdown of military personnel and reliance on sophisticated equipment have made the armed forces dependent on civilian specialists, be they government employees or contractor technicians." *Citations omitted*);

contractors in Afghanistan and Iraq actually surpassed the number of military forces and federal civilian employees.[198]

Contractor support growth also appears to have been partly driven by the chilling effect of modern media showing images of fallen soldiers. In a day and age where news of war has been streamed into households via television and internet 24 hours a day, some commentators have noted that many of our military decisions are more concerned with force protection than power projection.[199] When the military is fighting wars that millions oppose, or perhaps view as not vital to national security interests, then the deaths of soldiers becomes less and less acceptable.[200] Following this line of reasoning, some argue that it should not come as any surprise that the U.S. would so heavily rely on contractors for much of the war effort; fewer soldiers placed in harm's way means fewer news stories about dead soldiers.[201]

Given the DoD's current state of contractor reliance, many commenters have called for stronger oversight of contracts and contractor performance.[202] Not

---

Office of the Under Secretary of Defense (Comptroller)/CFO, United States Department of Defense, Fiscal Year 2012 Budget Request: Overview (2011), at 5-9 ("Contractors have been essential to supporting U.S. combat operations since they began in 2001. Contractor support allows our military to focus on operational missions. Additionally, the downsizing of our military after the end of the Cold War included significant reductions to military logistical and other support personnel. Contractors fill the resulting shortfalls in support"); Schmitt, *Humanitarian Law, supra note* 192, at 518 ("An additional motivator is that the technology of modern warfare often exceeds the ability of militaries to train their personnel… military purchases not only the weapon system, but also contracts for training and maintenance support, and, in some cases, even operation of the system." Citations omitted).

[198] CWC Final Report, *supra* note 2, at 18 (The CWC identified an in-theater, contractor workforce of 260,000 supporting Department of Defense, Department of State and U.S. Agency for International Development (USAID) missions). *See also* Blizzard, *Contractors on the Battlefield, supra* note 192, at 6 (according to Lt Col Blizzard, the U.S. military has relied heavily on civilians and contractors in the theater of war since the American Revolution. From World War II to the Balkan conflict of the 1990s, the ratio of civilians/contractors to military personnel in theater has not been below a 1:7 ratio, with the exception of Operations Desert Shield & Desert Storm, which were conducted by almost 100% military personnel.)

[199] Scott M. Sullivan, *Private Force / Public Goods*, 42 Conn. L. Rev. 853, 883 (2010), citing Jeffrey Record, *Force-Protection Fetishism: Sources, Consequences, and (?) Solutions*, Air & Space Power J. (Summer 2000), at 4-6 (Noting U.S. defense decisions very often "reflected a desperate unwillingness to place satisfaction of US armed intervention's political objective ahead of the safety of its military instrument.").

[200] *Id.*

[201] Unfortunately, the deaths of contractors in Iraq and Afghanistan do not seem to be as tragic and newsworthy to the media as the death of uniformed military. While the injuries and deaths of American troops have received a significant amount of coverage on television, in newspapers and magazines, and through online media, reports on contractor casualties have been minimal. *See* Steven L. Schooner & Colin D. Swan, *Contractors and the Ultimate Sacrifice* (Sep. 1, 2010) Service Contractor, p. 16, September 2010; GWU Legal Studies Research Paper No. 512; GWU Law School Public Law Research Paper No. 512, *available at* http://ssrn.com/abstract=1677506.

[202] *See generally* Steven L. Schooner & David J. Berteau, *Emerging Policies and Practice Issues* (2010), Public Law and Legal Theory Working Paper No. 529, Legal Studies Research Paper No.

surprisingly, in the UAS community, contractors also have been critical of extending their roles to mission execution. UAS technology is unmatched in its ability to provide power projection capability while supplementing force-protecting efforts.[203] However, it is exactly the highly technical, manpower intensive nature of this extremely long spear that raises questions about the role of contractors. Most importantly, the following questions need examination for compliance under current law and policy regarding the performance of inherently governmental functions: (a) whether UAS systems are being maintained and operated in a compliant manner, and (b) whether the imaging and data is being captured, analyzed and disseminated in a compliant manner.

B. The Role of Contractors in the Current UAS Mission

The important roles that contractors would play in UAS missions developed early in the current conflicts. For example, the Air Force was taking the Global Hawk to battle for the first time and was not ready to handle the job alone.[204] In the rush to field ISR assets to support Operations Enduring Freedom (OEF) and Iraqi Freedom (OIF), contractors comprised the majority of teams deployed to maintain and operate unmanned aircraft.[205] In short, the military simply did not have enough trained military personnel to handle the job unaided.[206] The UAS mission was

529 (2011) at 9-9, citing Vernon J. Edwards, *Contracting for Services: Challenges for the Next Generation*, 24 N&CR ¶ 59 ("It seems unlikely that in the current economic and political climate the Government is going to significantly reduce its reliance on contractor services in the near term. Thus, the problem must be managed.").

[203] With the majority of our aircrew and intelligence teams located in secured military bases in the continental U.S., the medium and large UAS keeps hundreds of military, civilian and contractor personnel out of harm's way. While it is possible that a strike could be launched against an installation such as Creech Air Force Base near Las Vegas, Nevada, or that a UAS crewmember could be targeted and attacked on his commute home or while shopping for groceries, the likelihood of combat related harm is negligible. Fewer pilots flying the skies of Iraq or Afghanistan mean fewer reports of downed Airmen. The American public does not shed tears when a drone goes down in a fiery crash.

[204] Blizzard, *supra* note 192, at 5-6 ("System contractors support deployed, operational forces under existing weapon system contracts. These contractors 'support specific systems throughout their system's life cycle (including spare parts and maintenance) across a range of military operations' (citing Joint Publication 4-0, Doctrine for Logistics Support of Joint Operations, Apr. 6, 2000, V-1). For example, the F-117A stealth fighter, reconnaissance aircraft, and Global Hawk unmanned aerial vehicle rely on system contractors for maintenance and logistics support").

[205] Michael J. Guidry & Guy J. Wills, *Future UAV Pilots: Are Contractors the Solution*, A. F. J. of Logistics, Winter 2004, at 5 (at the beginning of OEF, 56 contractors deployed as part of 82 member Global Hawk team to provide maintenance and operation of UAS during combat missions; similar contractor-military UAS workforce were used for OIF).

[206] The critical need for contractors to support the UAS mission was recognized in official planning documents. *See generally* Dep't of the Air Force, U.S. Air Force Remotely Piloted Aircraft and Unmanned Aerial Vehicle Strategic Vision [hereinafter Air Force Strategic Vision] (2005), at 19, *available at* http://www.globalsecurity.org/military/library/policy/usaf/afd-060322-009.pdf. ("the Air Force may supplement uniformed RPA and UAV pilots, logisticians, and maintainers with civilian employees or contractors. Such a decision will require careful consideration of what functions are "inherently governmental" and thus not subject to contracting out.").

growing, the inventory and capabilities were expanding exponentially, and the DoD reliance on contractors to support the mission was rising.[207] Given the shortfalls that DoD is experiencing with personnel, the military will not be able to free itself from dependence on contractors.[208] Therefore, it is critical that steps be taken to prevent contractors from performing functions that should not be outsourced, such as the offensive combat functions of UAS.[209]

1. The Kill Chain

The standard UAS combat air patrol (CAP) mission consists of six principal steps—find, fix, track, target, engage, and assess (F2T2EA), also known simply as the "kill chain."[210] Often referred to as "dynamic targeting," these six steps represent the linear sequence of events that are used by mission controllers and analysts conducting any mission that is prepared to engage targets of opportunity, for example, time sensitive targets such as a meeting of al Qaeda leadership.[211] Whether the mission involves attacks against planned targets, monitoring of areas suspected of enemy presence, or general reconnaissance—the process is basically the same.

---

[207] U.S. Gov't Accountability Office, GAO-08-1087, Military Operations: DOD Needs to Address Contract Oversight and Quality Assurance Issues for Contracts Used to Support Contingency Operations 29 (2008) ("For the contracts we reviewed, DoD used contractors to support contingency operations for several reasons, including the need to compensate for a decrease in force size and a lack of capability within the military services. For example, in fiscal year 2002, Congress provided the Air Force with $1.5 billion to acquire 60 additional unmanned Predator aircraft; however, according to Air Force documents, the Air Force did not have the additional 1,409 personnel needed to maintain these new assets. As a result, the Air Force used contractors to support the additional aircraft."); Bill Sweetman, *Next UAV Contractors Will Need New Skills*, Aviation Week, Jul. 1, 2010, *available at* http://www.aviationweek.com/aw/generic/story.jsp?topicName=unmanned&id=news/dti/2010/07/01/DT_07_01_2010_p42-236479.xml&headline=Next%20UAV%20Contractors%20Will%20Need%20New%20Skills&channel=&from=topicalreports (stating that the proprietary nature of many unmanned systems has furthered dependency on the UAV manufacturers who secure contracts for significant follow-on support).

[208] Cloud, *Civilian Contractors, supra* note 1.

[209] *See e.g.*, Fontaine & Nagl, Contracting in Conflicts, *supra* note 131, at 25-26 (Stating there is a questionable legal status of contractors "carrying out functions more closely related to military activities, such as intelligence collection and support, logistics support to forward deployed troops, operating drones, maintaining or repairing weapons systems, or (possibly) using a weapon, even if fired in self-defense."); *see also* Guidry & Wills, *supra* note 205, at 9-13; Blizzard, *supra note* 192, at 10 (arguing that UAV piloting is direct participation in hostilities and could subject the contractor pilots to prosecution as criminals); Air Force Instruction 11-502, Vol. 3, Flying Operations: Small Unmanned Aircraft Systems Operations, Apr. 26, 2012, at ¶4.1 ("To ensure the noncombatant status of civilians and contractors is not jeopardized, commanders shall consult with their servicing judge advocate office for guidance before using civilian or contractor personnel in combat operations or other missions involving direct participation in hostilities.").

[210] Lt Col Recker Interview, *supra* note 68.

[211] Office of the Joint Chiefs of Staff, Department of Defense, Joint Publication 3-60: Joint Targeting (Apr. 13, 2007), at II-12 (The F2T2EA sequence is used for both missions that engage targets developed during deliberate targeting, where known targets are previously identified for prosecution, or dynamic targeting, which engages targets of opportunity that arise) *available at* https://jdeis.js.mil/jdeis/new_pubs/jp3_60.pdf.

With one or more aircraft, the remote ground station operators and analysts pour over video feeds, images, and data streamed from the aircraft to "detect objectives of potential significance," that is, *find* the target[212] Once identified, operators and analysts use the UAS mapping and advanced sensors to get a fix on the target, that is, determine the target's precise location. Once the target's location is established, then operators and analysts will continue to monitor (i.e., *track*) the target. While tracking the target, they will collect more data regarding the target and the target's movements; the surrounding environment, vehicles, buildings and residences; and patterns of life and movement (including the presence and activity of other people in the immediate area who might be subject to harm).[213]

At this stage of the mission, the focus shifts from what might be considered passive surveillance to active coordination—with ground troops who will confront the target or with the execution of kinetic air strikes against the target. Based on intelligence collected and analyzed, mission commanders decide upon resources that will be used against the target (now truly a *target*).[214] Military ground forces and/or UAS kinetic capabilities are applied against the target in a timely and decisive manner.[215] Meanwhile, still circling above the target, the UAS aircraft is there to *assess*.[216] Did the ground troops capture or kill the target? Did the missile take out the building? How much damage was done to the surrounding area? Were any innocent civilians harmed? And perhaps, most important for a military mission, does the target need to be attached again?[217]

As previously mentioned, getting an aircraft and ground control equipment ready to conduct such missions; operating the sensors and aircraft in flight; and collecting, processing and disseminating intelligence necessary for the mission can involve hundreds of people, many of whom are contractors. Many in the UAS community believe contractors play important roles in UAS sustainment and missions, but are not within the kill chain. Accordingly, the question arises, what

---

[212] Mark K. Waite, Increasing Time Sensitive Targeting (TST) Efficiency Through Highly Integrated C2ISR, Research Report submitted to fulfill degree requirements at the Air Command and Staff College (2002), at 28 *available at* http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA420652&Location=U2&doc=GetTRDoc.pdf.

[213] *Id.*

[214] *Id.*

[215] *Id.*

[216] *Id.*

[217] The kill chain is not isolated to the large and medium UAS. Testifying before House Oversight and Government Reform Subcommittee on National Security and Foreign Affairs in 2010, Michael S. Fagan, Association of Unmanned Vehicle Systems International (AUVSI) provided written statistic showing how critical employment of small UAS has become for Army commanders. Approaching one million flight hours as of March 2010, Army UAS were "predominantly employed as tactical Reconnaissance, Surveillance, and Target Acquisition (RSTA) platforms supporting the Commander's scheme of maneuver. In this role, Army UAS have filled a critical need, providing 'actionable' intelligence and decreasing the time between sensor and shooter (shortening the 'kill chain')"). *See Rise of the Drones I, supra* note 19 (statement of Michael S. Fagan).

activities are within the kill chain? For example, is the kill chain limited to the person releasing a Hellfire missile, or does the kill chain include other actors supporting "combat" or the "direction and control of intelligence?" In the following sections, the functions that contractors are (or may be) performing—and the relation of those functions to the kill chain—are examined. This examination analyzes the question of what should not be contracted because the function is inherently governmental or for other policy reasons.

2. Logistics and Maintenance

(a) *The Blended Maintenance Workforce*

Generally, few regard the maintenance and repair of aircraft, sensors, and communications systems as inherently governmental activities. For the last several decades, civilian contractors have provided such maintenance and repair services, typically working alongside military and federal civilian counterparts as a team, often doing the same type of work, sometimes indistinguishable in appearance to outsiders. It is this reliance on contractors for so many important functions such as maintenance and repair of weapons systems, and the recognition that the U.S. will not completely abandon such a "blended" workforce in the current political environment, that demands this workforce be well managed.[218] An important step in pursuing management of these has been the publication of DoD guidance and regulations to address the complications that arise between the military personnel and the contractors working in the same organizations, as well as the specific work that can be performed by contractors in regard to military aircraft, payloads, and armament.[219]

(b) *Battlefield Contract Maintenance*

DoD dependence on contractors has not been limited to their employment back in the U.S. As part of the recognized blended workforce, contractor maintenance

---

[218] *See generally* Schooner & Berteau, *supra* note 202, at 9-9.

[219] *See generally* Defense Contract Management Agency Instruction 8210.1, Contractor's Flight and Ground Operations, Mar. 1, 2007, *available at* http://guidebook.dcma.mil/227/Contractors_Flight_and_Ground_Operations.htm; Dep't of the Army, Army Tactics, Techniques, and Procedures 4-10: Operational Contract Support Tactics, Techniques, and Procedures, Jun. 20, 2011, *available at* https://armypubs.us.army.mil/doctrine/DR_pubs/dr_aa/pdf/attp4_10.pdf (this 2011 publication represents the latest guidance on modern Army contractor management, that originated with the 1999 publication of Field Manual (FM) 100-10-2: Contracting Support on the Battlefield, and the 2000 publication of FM 100-21: Contractors on the Battlefield); Air Force Materiel Command Guide for the Government-Contractor Relationship, Oct. 2006, *available at* www.acq.osd.mil/dpap/ccap/cc/jcchb/.../gov.ctr.relationshipaf.doc (recognized by all services as a helpful resource for government personnel responsible for managing blended teams of military, federal civilian, and contractor employees); Report of the Acquisition Advisory Panel, *supra* note 92, at 389-426 (In *Chapter 6: Appropriate Role of Contractors Supporting Government*, the Panel provides an extremely helpful discussion of personal services contracts, organization conflicts of interest, and personal conflicts of interest).

teams have deployed with military forces to theaters of war for the last decade to maintain fielded weapons systems.[220] Key weapons systems maintenance contractors are specifically identified by the DoD as contractors authorized to accompany the armed forces.[221] Some scholars, however, have questioned the legality of contractors performing battlefield weapons systems maintenance. Many argue that contractors providing maintenance and repair of weapons in an area of conflict, in certain situations should be considered direct participation in hostilities.[222] As previously discussed, direct participation in hostilities by civilians is prohibited

---

[220] *See e.g.,* Blizzard, *supra* note 192, at 6 (noting that contractors handled 28 percent of weapons systems maintenance, even though the Bush administration wanted to increase contractor responsibility to 50 percent); Guillory *supra* note 182, at 123-24 (discussing the numerous contractors deployed in support of highly technical, modern weapons systems); Douglas, *supra* note 187, at 133-34 ("The third type of battlefield contract is a system contract for the support and maintenance of equipment throughout the system's lifecycle. Such systems include vehicles, weapon systems, and aircraft and communications systems deployed with the military." *citations omitted*); Report of the Acquisition Advisory Panel, *supra* note 92, at 416 ("[I]n recent years, the military has become dependent upon contractor support for transportation, shelter, food, and 'unprecedented levels of battlefield and weaponry operation, support, and maintenance.' (citing Schooner, *Contractor Atrocities, supra* note 4, at 554) Additionally, the DoD has 'encouraged the procurement of complex defense systems under contracts requiring ongoing contractor support throughout the systems' life cycles.' (citing Vernon, *Battlefield Contractors, supra* note 170, at 374); GAO-08-1087, *supra* note 207, at 1 (describing the numerous jobs performed by the tens of thousands of contractors in Iraq and Afghanistan, to include weapons systems maintenance).

[221] Dep't of Defense of Instruction 3020.41, Contractor Personnel Authorized to Accompany the U.S. Armed Forces, Oct. 3, 2005, ¶E2.1.15.

Although use of contractors is widely accepted, many also recognize that it is imperative the military branches possess the core capacity to maintain critical weapons using organic capabilities. *See generally* Sullivan, *supra* note 199 at 887-8 (finding that the DoD relied heavily on contractors to provide critical specialized skills and expertise needed for maintenance of complex military machinery and weapons systems); Frank Camm & Victoria A. Greenfield, RAND, How Should the Army Use Contractors on the Battlefield? Assessing Comparative Risk in Sourcing Decisions (2005), at 181, *available at* http://www.rand.org/pubs/monographs/MG296.html (cautioning that analysis of core activities should "start with the opportunity a contract source offers and then look for valid reasons to avoid using a potentially attractive source"); Sandra I. Irwin, *Pentagon Insourcing Fueling Contractor Anxiety*, Nat'l Def., Apr. 2011, *available at* http://www.nationaldefensemagazine.org/archive/2011/April/Pages/PentagonInsourcingFuelingContractorAnxiety.aspx (stating that the Defense Department expects to insource more weapon maintenance and repair work because, under current laws and policies, it must have a core capacity to fix critical systems in house).

[222] *See generally* Schmitt, *Humanitarian Law, supra* note 192, at 544-545 ("Depot maintenance of military equipment, in other words, maintenance conducted away from the battle zone, is relatively remote from the hostilities and clearly not direct participation. Similarly, routine, regularly scheduled maintenance on equipment, even near the front, does not directly impact on specific operations. On the other hand, preparing equipment for battle has a direct impact on the course of battle. Thus, activities such as fueling aircraft, loading weapons, conducting preflight checks, performing life-support functions, and locally repairing minor battle damage would meet the direct participation threshold. Between these two extremes, as with all other cases cited above, the analysis must be case specific."); Blizzard, *supra* note 192, at 9 (stating that contracted Predator and Global Hawk maintenance, and ISR systems operations, puts civilian contractors at risk of crossing the line into "unlawful direct participation in hostilities"); Camm & Greenfield, *supra* note 221, at 159-60 (describing the wide spread disagreement that exists among legal experts as to the support activities contractors can perform in a theater of war and retain lawful noncombatant status).

under international law. Such direct participation costs a civilian all protections under LOAC such as protection from lawful attack, POW status if captured, and combatant immunity from prosecution.[223]

(c) *Battlefield Contract Maintenance and Inherently Governmental Functions*

Both OFPP Policy Letter 11-1 and DoDI 1100.22 reinforce the DoD's position that weapons systems maintenance and repair are not inherently governmental, but rather activities that can be performed by a blended workforce without violating LOAC. First, DoDI 1100.22 specifically identifies weapons systems maintenance, occurring even at forward operating bases during contingency operations, as a function that can be performed by contractors if there is insufficient military manning or expertise available to perform the activity: "if a Military Service has a new weapon system available for use during hostilities, but sufficient numbers of military maintainers are not yet trained, the commander might be able to use contract maintenance in a secure compound without degrading the operational capability of the system."[224] Second, while activities listed in OFPP policy letter are illustrative and non-exhaustive, it should be noted that maintenance and repair activities are not identified in its Appendix A as inherently governmental, or in its Appendix B as closely associated with inherently governmental.[225] Further, the introductory passages to the OFPP Letter 11-1 demonstrate clearly that the omission of weapons systems maintenance from the Appendices was intentional rather than oversight—OFPP simply did not agree with all comments received when OFPP Letter 11-1 was proposed.[226] Weapons systems maintenance, nevertheless, could arguably be regarded as a critical function, that is, "a function that is necessary to the agency being able to perform and maintain control of its mission and operation."[227] While such positions may be filled by government or contractor personnel, agencies must retain sufficient internal capability to maintain control over the mission and operations through (1) an adequate number of "Federal employees with appropriate training, experience, and expertise" and (2) internal ability to oversee and manage the contractor workforce.[228]

---

[223] *See supra* notes 189-91.

[224] DoDI 1100.22, *supra* note 144, at 21.

[225] OFPP Policy Letter 11-1, *supra* note 128 at 56240-56241.

[226] *Id*. at 56229 ("One form letter, submitted by approximately 30,000 respondents, expressed concern about excessive outsourcing and recommended expanding the definition of an inherently governmental function to encompass critical functions and closely associated functions. The letter also proposed augmenting the list of inherently governmental functions to include all security functions and intelligence activities, training for interrogation, military and police, and **maintenance and repair of weapons systems**.") (emphasis added).

[227] *Id.* at 56236 (one should note that while OFPP Policy Letter 11-1 states that "facilities maintenance" is ministerial in nature and not inherently governmental, weapons systems maintenance varies significantly from facilities maintenance, and understandably involves more important and more DoD-specific technology than standard plumbing, electrical, or carpentry.).

[228] *Id.* at 56238.

(d) *Contracted UAS Maintenance*

Deployed contractors proved particularly necessary for sustainment of the hundreds of UAS aircraft, sensors and ground station equipment used in Iraq and Afghanistan.[229] In 2005, the Air Force spent slightly less than $50 Million annually for contractor maintenance of just MQ-1 Predators.[230] As of May 2009, 75 percent of Air Force MQ-1 Predator and MQ-9 Reaper maintenance requirements were handled by contractors; 100 percent of Air Force Special Operations Command maintenance requirements were executed by contractors.[231] Similar contractor maintenance support was required for the Army and Marine UAS operations.[232]

(e) *UAS Battlefield Contract Maintenance*

While the foregoing contractor reliance may appear excessive, the U.S. military's use of contractors for UAS systems maintenance adheres to the current policy on inherently governmental and critical functions, as well as relevant DoD regulations. The Air Force has taken steps to implement the guidance offered in OFPP 11-1 and DoDI 1100.22 for using contractors for UAS maintenance. First, the Air Force has instituted UAS maintenance training programs at Sheppard Air Force Base. There, Airmen receive fundamental aircraft repair training and prepare for subsequent system specific training. This training was established, in part, in recognition that operations must be sustainable in the event that contractors are not

---

[229] *See* Mike Alberts, 25th Combat Aviation Brigade Public Affairs, *Task Force Wing's Hunter Provides 'Eyes and Ears' on the Battlefield in Northern Iraq*, March 30, 2010, *available at* http://www.army.mil/article/36588/ (discussing Army reliance on contractors to maintain Hunter UAS); Blizzard *supra note* 192, at 9 (discussing the Air Force's heavy use of contractors for Predator/Global Hawk maintenance); Guidry & Wills *supra* note 205 at 5 (stating that contractors deployed early in OEF to provide maintenance of Global Hawk). The author also had the opportunity to interview Mr. Jim Ryan, Headquarters, Department of the Army, Operations, Plans, and Training (Unmanned Aviation), HQDA DCS G-3/5/7, on Dec. 11, 2011 [hereinafter Ryan Interview], who informed him that contractors are used for Army UAS maintenance and operations when "a qualified soldier does not exist (new sensor/aircraft type), when there is insufficient quantities of trained soldiers, when its advantageous for Force Cap considerations and when the Contractor can provide enhanced maintenance (Field Service Reps that don't void warranty items)."

[230] GAO-08-1087, *supra* note 207, at 17.

[231] Dep't of the Air Force, United States Air Force Unmanned Aircraft Systems Flight Plan, 2009-2047 (May 18, 2009) [hereinafter UAS Flight Plan, 2009-2047], at 77, *available at* http://www.globalsecurity.org/jhtml/jframe.html#http://www.globalsecurity.org/military/library/policy/usaf/usaf-uas-flight-plan_2009-2047.pdf.

[232] Dep't of the Army, Field Manual 3-04.155, Army Unmanned Aircraft System Operations (July 2009), at 1-5 – 1-9, *available at* https://armypubs.us.army.mil/doctrine/DR_pubs/dr_c/pdf/fm3_04x155.pdf (identifying the embedded contractor logistics support required to maintain the Army's RQ-7B Shadow, Warrior-A, MQ-5B Hunter and MQ-1C Quick Reaction Capability aircraft—the Gray Eagle predecessor); Office of the Deputy Commandant for Aviation, United States Marine Corps, FY2011 Marine Aviation Plan [hereinafter Marine Aviation] (Sep. 2010), at 6-2 & 11-7, *available at* http://www.aviationweek.com/media/pdf/Check6/FY11MarineAviationPlan.pdf (describing the Marine Corps plan to transition away from contractor reliance on the Insitu Scan Eagle contractor-owned, contractor-operated (COCO) platform).

available.[233] Second, the Air Force is staffing the current theaters of operations with well-balanced maintenance teams comprised of approximately half military and half contractor (the majority of which being former military).[234] In so doing, the Air Force maintains sufficient control over maintenance operations and the contractor workforce.[235] Contractors continue to play an important role in UAS maintenance, but the Air Force has made substantial progress with, and continues to foster the growth and development of its internal capability.

The Army, although it has depended heavily on contract maintenance to sustain its fielded UAS,[236] similarly has made significant progress in developing trained military mechanics to support its rapidly expanding UAS inventory.[237] With a goal of contractors providing only 20 percent of all necessary UAS maintenance,[238] the Army has stood up maintenance training programs a Fort Huachuca, Arizona for its RQ-5 Hunter and MQ-1C Gray Eagle UAS.[239] In comparison, the Navy and Marines have trailed their sister services in the development of these core UAS capabilities. As a result, the two have relied more heavily on contractors for both operations and maintenance.[240] The Navy intends to address its need for military maintainers through training programs at the Naval Air Station (NAS) Jacksonville and Beale Air Force Base for the MQ-4C BAMS, and at NAS North Island for

---

[233] Henry Canaday, *Unmanned but Well Supported*, Military Logistics Forum, Vol 4, Issue 7 (Aug. 2010), at 18, 20; Interview of Major Casey Tidgewell, AF/A3O-AC, conducted on Dec. 21, 2011 [hereinafter Major Tidgewell Interview]; Interview of Chief Master Sergeant Mark Kovalcik, 2A3/2A5/2R Career Field Manager, HQ USAF/A4LF, conducted on Jan. 5, 2012 [hereinafter Chief Kovalcik Interview].

[234] *Id.;* Bill Yenne, *Birds of Prey, supra* note 9, at 71-83; *The Future of Unmanned Air Power, supra* note 67 (noting that the majority of maintenance performed on the UAS aircraft is provided by the blended military-contractor field teams at overseas military bases, to include four sites in Iraq and Afghanistan).

[235] UAS Flight Plan, 2009-2047, *supra* note 231, at 29, 77 ("[T]he UAS maintenance community is proactively developing long-term normalization plans that meet Joint requirements while balancing USAF manpower goals. Presently all Global Hawk organizational-level maintenance is military "however future forward operating locations (FOLs) are planned to be contract maintenance." In the case of MQ-1/9 however, 75% of ACC and 100% of AFSOC organizational level flight line maintenance requirements are performed by contractors. HAF/A4/7 and HQ ACC both favor 100% replacement of organizational level flight line contractors with funded military authorizations.")

[236] Ryan Interview, *supra* note 229 (stating the Army has experienced "heavy augmentation of contractors for [UAS] maintenance and PED during wartime.").

[237] GAO 10-331, *supra* note 62, at 11 (crediting the Air Force and Army efforts to train personnel to operate UAS aircraft and perform maintenance, but finding that the services "have not yet fully developed strategies that specify the actions and resources required to supply the personnel needed to meet current and projected future UAS force levels").

[238] Army Roadmap, *supra* note 45, at 41.

[239] Major Tidgewell Interview, *supra* note 233; Lt Col Cutting Interview, *supra* note 52 (explaining that the Army maintenance training pipeline is designed to accommodate up to 625 UAS "Repairer" students each fiscal year who begin with a 17 week introductory program, and then progress to follow on training for their specific UAS. Secondary training for the Hunter is a 27 week program, whereas the Gray Eagle will demand 35 additional weeks).

[240] Marine Aviation, *supra* note 232.

the MQ-8B Fire Scout.[241] The Marines will continue to use contractor-owned/ contractor-operated (COCO) systems, and the Corps intends to work jointly with the Army at the Fort Huachuca training centers to obtain operator and maintenance training for its RQ-7B Shadow and RQ-11B Raven UAS inventory.[242]

(f) *Military Preferred, but Contractors Allowed*

Although some scholars regard battlefield maintenance—to include arming weapons systems—as direct participation in hostilities, there are several nations, to include the United States, that opine that contracted battlefield maintenance generally does not cross the line into unlawful belligerent activity.[243] As Professor Geoffrey Corn notes, "[t]he increasing technological complexity of weapons systems often requires civilian technical experts to maintain these systems. Even if the maintenance of weapons systems is considered to fall within the realm of application of combat power, the exercise of discretion related to this function involves no reasonable probability of a LOAC violation. Accordingly, civilianization is permissible."[244] In short, a weapons systems operator decides "when and where to engage an enemy;" the individual who readies that weapons system simply does not possess the discretion to apply combat power.[245]

While the services are striving to train UAS maintainers, such core capability cannot be achieved overnight so a contractor workforce will continue to be necessary.

---

[241] Major Tidgewell Interview, *supra* note 233.

[242] *Id.*; Marine Aviation, *supra* note 232; *see also* U.S. Gov't Accountability Office, GAO-11-673, Army and Marine Corps Training: Metrics Needed to Assess Initiatives on Training Management Skills 11 (2011) (stressing that joint training centers are critical considering that in the past, both Army and Marine units were "often unable to integrate unmanned aerial systems into training prior to arriving at the combat training centers" just prior to deployment.).

[243] *See generally* Daphné Richemond-Barak, *Private Power and Human Rights: Rethinking Private Warfare*, 5 Law & Ethics Hum. Rts. 159, 162, 186-190 (May 2011) (providing a detailed discussion of the *Montreux Document*, a non binding international document "[s]igned in 2008 by 17 states, and endorsed by an additional 18 states since its release," which represents "the first international document seeking to regulate the conduct of military and security companies involved in armed conflicts," to include "armed guarding and protection of persons and objects, such as convoys, buildings and other places; maintenance and operation of weapons systems; prisoner detention; and advice to or training of local forces and security personnel." (*citations omitted*)).

[244] Corn, *Unarmed, supra* note 187, at 291.

[245] *Id.; see also* Memorandum from Mary Walker, General Counsel, Office of the Secretary of the Air Force (SAF/GC), to Secretary of the Air Force for Acquisition (SAF/AQ) and Deputy Chief of Staff for Plans and Operations, United States Air Force (AF/XO) (June 9, 2005) (on file with author) (concluding that contractors performing UAV weapons systems maintenance and loading munitions are not violations of LOAC since these "specific activities of the contractor . . . are not likely to cause actual harm to an adversary," unlike the actions of the UAV pilot. Similarly, in accordance with the DoDI 1100.22 "manpower mix criteria," these activities should not be considered inherently governmental because "(1) use of deadly force is not required as an inherent part of the operation to be performed by the contractor; (2) UCMJ authority and discipline and military training are not normally required for proper performance of the duties; and (3) performance of the function by contractors does not constitute an inappropriate or unacceptable risk.").

Contractors deployed for weapon systems maintenance operate out of established overseas military installations or highly secured forward operating bases. Essentially, most of the work they are performing overseas is the same they would perform on a base back in the U.S. The contractor does not grab a rifle, throw his tools in a rucksack, and head into the thick of battle with a military unit on combat patrol.[246] Rather, the contracted maintainers are positioned at secured facilities where a wide array of logistics support is generated.[247] Although weapons systems maintenance is critical—hence, the services' efforts to train sufficient numbers of military personnel—it is not inherently governmental and maintainers should not be thought of as participants in hostilities.

3. Intelligence Analysis

(a) *The Current Debate on Contracted Intelligence*

Who can perform intelligence activities for the U.S. government is a question that has been the subject of much debate.[248] Despite possible opposition, however, the DoD has relied quite extensively on contract support for intelligence operations.[249] The FAR, DoDI 1100.22, and OFPP Policy Letter 11-1 each regard the "direction and control of intelligence and counter-intelligence operations" as

[246] Guillory, *supra* note 182, at 134-35. ("[W]eapons system technicians who have a "habitual relationship" with combat troops to the extent that they deploy with them to the "foxholes" or "downrange" would be performing combatant activities. However, technicians occasionally travelling to a missile silo in the continental United States or to the frontline to perform maintenance or repairs on a weapons system would lack the requisite integration, and therefore remain lawful noncombatants." (*citations omitted*)).

[247] Email sent to author from Mr. Jim Ryan, HQDA DCS G-3/5/7, Dec. 22, 2011, on file with author. [hereinafter Ryan Email] (writing "UAS Contactors fulfill support roles as Pilots/Operators, Maintainers, Instructors and exploiters. Before launching into individual airframe discussion here are some helpful business rules for use of contactors on Army UAS. 1. Contactors do not fire, or terminally guide munitions (includes laser, Electronic Warfare or any kinetic effect.) 2. Contactors do not leave the wire (Operate while deployed only from US Bases, no going on patrols).").

[248] Compare for example Walter Pincus, *Increase in Contracting Intelligence Jobs Raises Concerns*, Wash. Post, Mar. 20, 2006, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/03/19/AR2006031900978.html (criticizing the U.S. Government's self-created necessity to use thousands of civilian contractors to perform intelligence and interrogation activities which may be inappropriate work for non-governmental workers) to Daniel Goure, Ph.D., Lexington Institute, *Washington Post Series Criticizing Intelligence Contractors Is Short On Evidence*, Early Warning Blog, July 20, 2010, *available at* http://www.lexingtoninstitute.org/washington-post-series-criticizing-intelligence-contractors-is-short-on-evidence?a=1&c=1171 (writing that the Washington Post is unrealistic in its criticism of contracted intelligence costs and incorrect in its suggestion that contractors are performing intelligence activities barred by law).

[249] Turner & Norton, *supra* note 187, at 22-23 (describing civilians in Iraq and Afghanistan "operating and managing intelligence and information systems"); Voelz, *supra* note 87, at 588 ("Some estimates identify as many as sixty private firms providing [the DoD] various security and intelligence-related services in Iraq and Afghanistan, though even the government has struggled to provide a precise accounting for all contractor activities (citation omitted)").

inherently governmental functions.[250] However, these resources do not define the term "direct and control," so that task is left to the agencies to address.[251] Not surprisingly, this question does not lead to a simple answer.

According to a paper released by the Office of the Director of National Intelligence (DNI) on July 19, 2010, "[t]he Intelligence Community does not condone or permit contract personnel to perform inherently governmental intelligence work, as defined by *OMB Circular A-76* . . . . Core contract personnel may perform activities such as collection and analysis; however, it is what you do with that analysis, who makes that decision, and who oversees the work that constitute the 'inherently governmental' functions."[252] Conversely, many scholars opine that participation in intelligence collection, particularly tactical intelligence, constitutes direct participation in hostilities, a status reserved for combatants under the laws of armed conflict.[253] Because of this possible link to a combat role, many scholars view tactical intelligence as inherently governmental.[254]

---

[250] FAR *supra* note 151; DoDI 1100.22 *supra* note 144; OFPP Letter 11-1 *supra* note 33.

[251] Shirk & Madon, *supra* note 129 (Noting that the importance of clarifying policy on inherently governmental functions was recognized in 2007 by members of the House Permanent Select Committee on Intelligence, who "reported they were 'concerned that the Intelligence Community does not have a clear definition of what functions are 'inherently governmental' and, as a result, whether there are contractors performing [sensitive] inherently governmental functions,'" citing H.R. Report No. 110-131, at 42 (May 7, 2007)).

[252] Office of the Dir. of Nat'l Intelligence, Key Facts About Contractors (2010), a*vailable at* http://www.dni.gov/content/Truth_About_Contractors.pdf.

[253] *See generally* Chesterman, *supra* note 103, at 1069 (concluding the simplest solution to prevent violations of the law of armed conflict would simply be to "forbid certain activities [such as intelligence operations] from being delegated or outsourced to private actors at all"); Christensen, *supra* note 186, at 281 (stating that "transmitting tactical intelligence," should not be performed by civilians, citing ICRC, Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law, at 47-49 (2009) [hereinafter ICRC, DPH Guidance], *available at* http://www.icrc.org/WeblEng/siteengO.nsflhtmlall/pO990/$File/ICRC_002_0990.PDF) Blizzard, *supra note* 192, at 135 (describing tactical intelligence collection intended "to disrupt enemy operations or destroy enemy forces or installations" as an activity that only combatants may perform); Heaton, *Civilians at War, supra* note 20, at 155 ("The rule that participation in activities closely associated with the direct infliction of violence is more likely to be labeled combat explains why activities such as gathering intelligence for targeting purposes and servicing a weapons system may be considered direct participation in hostilities," citing Hans-Peter Gasser, *Protection of the Civilian Population*, in Fleck, *supra* note 169, at 232; Schmitt, *Humanitarian Law, supra* note 192, at 534 ("Consider intelligence. Rendering strategic-level geopolitical estimates is certainly central to the war effort, but will have little bearing on specific combat missions. By contrast, tactical intelligence designed to locate and identify fleeting targets is the *sine qua non* of time-sensitive targeting; it is an integral component of the application of force against particular targets. Civilians providing strategic analysis would not be directly participating in hostilities, whereas those involved in the creation, analysis, and dissemination of tactical intelligence to the "shooter" generally would.").

[254] *Id.*

(b) *Contracted Intelligence Activities within UAS Missions*

The DoD appears to have adopted a position similar to that of the Office of the DNI, but is not quite as dependent on contractors for intelligence activities. When asked about the roles contractors were playing in UAS intelligence operations, Mr. Charles Blanchard, Air Force General Counsel, responded, "[t]here might be a few civilian or contractor analysts, intelligence analysts who are doing imagery analysis."[255] At this time, there are approximately 80 to 90 personnel involved in intelligence processing, exploitation and dissemination (PED) for each MQ-1 Predator or MQ-9 Reaper CAP; there are approximately 300 personnel involved in PED for each RQ-4 Global Hawk CAP.[256] While the number of individuals required for PED may seem high, most of the individuals performing this intelligence role are military personnel. According to the Air Force RPA Task Force, the programmed end strength for PED manpower for Fiscal Years 2011, 2012 and 2013 is approximately 5000 personnel.[257] Of total end strength numbers, however, around 10 percent of the manning requirements are projected to be filled by government civilians or contractors.[258] The remaining assignments are projected to be filled by military personnel.[259]

Because of the critical importance of the UAS intelligence mission, the Army likewise has utilized contractor analysts to address manpower shortages and supply expertise.[260] To address pressing Operation Iraqi Freedom (OIF) intelligence needs, in 2006, the Army deployed a government owned/contractor operated (GOCO) MQ-5A Hunter unit.[261] Since that time, the Army has amassed

---

[255] *Drones, Remote Targeting, and the Promise of Law* (New America Foundation Discussion Panel Feb 24, 2011) at 1:13:51, *available at* http://www.ustream.tv/recorded/12909598 [hereinafter *Drones Promise*] (statement of Charles Blanchard) (additionally recognizing that contractors may have a role as linguistic interpreters and in launch and recovery operations).

[256] *The Future of Unmanned Air Power, supra* note 67; Lt Col Recker Interview, *supra* note 68 (noting that for Predator and Reaper CAPs, approximately 45% of the 180 to 200 person crew are involved in PED; for the Global Hawk, approximately 65% of the 450 to 500 CAP mission personnel perform PED).

[257] *The Future of Unmanned Air Power, supra* note 27, at 24:37 (statement of Lt. Col. Bruce Black) (indicating that for the Air Force to operate at a steady state of 65 CAPs with full manning requirements, the service would require 12,000 personnel, of which 5400 would perform PED).

[258] *Id.*; Hughes Interview, *supra* note 78. *See also* Cloud, *Civilian Contractors, supra* note 1 (Writing that the Air Force Special Operations Command "said in a statement that it employs 165 civilians to analyze video and other intelligence," and that "[a]n additional 300 civilians support other Air Force drones at 10 military bases in the U.S., Germany and South Korea.").

[259] *Id. See also* Cloud, *Civilian Contractors, supra* note 1 (reporting that the "Air Force is rushing to meet the [manning] demand." Regarding intelligence manning requirements, the Air Force "converted seven Air National Guard squadrons into intelligence units to help analyze drone video. About 2,000 additional Air Force intelligence analysts are being trained.")

[260] Field Manual 3-04.155, *supra* note 232, at 3-18 ("The most important factor regarding UAS employment is the effective, timely, and focused dissemination and exploitation of UAS information.").

[261] Army Roadmap, *supra* note 45, at 45.

a substantial inventory of unmanned assets that will be supported by military and contractor personnel. Due to rapid fielding and manning shortages, the Army has "established several Government Owned Contractor Operator detachments to assist in meeting theaters insatiable appetite for ISR," where contractors augment "[s] oldiers flying, maintaining and some exploitation."[262]

Contractors provide the backbone for current Navy and Marines UAS intelligence missions and analysis. The Marines, in particular, rely heavily on contractors to conduct missions for both the Marine owned and operated RQ-7 Shadow and the contractor-owned/contractor operated (COCO) Insitu Scan Eagle. For both platforms, one of the most significant limitations in establishing robust support for ground forces has been "a lack of trained intelligence analysts, UAS mission commanders, and maintenance personnel."[263] Of all military branches, the U.S. Navy has conducted the fewest UAS operations in current theaters of war. Although contractors operate the BAMS and MQ-8B Fire Scout, the Navy primarily uses military intelligence analysts for strategic and tactical ISR missions.[264]

(c) *Retaining Control over Contracted Intelligence*

While each branch seeks to control intelligence activities, no service seeks to eradicate contractor performance of PED functions. With regard to the Air Force, the 10 to 1 (possibly as high as 8 to 1) ratio between military and contractor intelligence personnel supports the view that the Air Force is making a conscious effort to retain control over intelligence analysis activities, and keeping contractors from engaging in inherently governmental activities.[265] In addition to the present workforce, the Air Force has "converted seven Air National Guard squadrons into intelligence units to help analyze drone video," and is currently training an additional

---

[262] Ryan Email, *supra* note 247.

[263] United States Marine Corps Center for Lessons Learned, Unmanned Aerial Systems (UAS) Integrated Operations in Support of Regional Command Southwest (RC (SW)), Oct. 4, 2011, at 3, *available at* http://publicintelligence.info/MCCLL-UAS-RC-SW.pdf.

See also Christopher Paul, Harry J. Thie, Katharine Watkins Webb, Stephanie Young, Colin P. Clarke, Susan G. Straus, Joya Laha, Christine Osowski, Chad C. Serena, RAND, Alert and Ready: An Organizational Design Assessment of Marine Corps Intelligence, Prepared for the United States Marine Corps, (2011), at 45-46, 70, *available at* http://www.rand.org/pubs/monographs/MG1108.html (identifying the need to build Marine UAS intelligence capability at the Company level and Air Combat Element).

[264] Naval Air Systems Command, *Fire Scout UAS Supports Operations in Afghanista*n [hereinafter NAVAIR *Fire Scout*], June 15, 2011, *available at* http://www.navair.navy.mil/pma266/pdfs/UAS_support.pdf (government owned/contractor operated Fire Scout deployed with a team including "a military [officer in charge (OIC) and assistant OIC, five Navy intelligence analysts, and 21 Northrop Grumman contractors to conduct missions in support" ISR needed for northern Afghanistan).

[265] Hughes Interview, *supra* note 78 (Stating that in regard to the ratio of military to civilian contractors performing intelligence analysis and PED functions, the ratios of "10 to 1, 8 to 1 is right in the ballpark." Even though he cannot supply actual numbers of personnel, Mr. Hughes stated that these ratios were representative of the blended intelligence workforce within Air Force UAS programs.)

2,000 Airmen to serve as analysts.[266] Similarly, the Army is seeking to impose restrictions on the use of contractors for intelligence activities. The Army uses contractors only when a qualified soldier does not exist, when there are insufficient quantities of trained soldiers, or when it is "advantageous to Force Cap [manning limitation] considerations."[267] Further, Army contractors "are always under direct military supervision and operate with/bound by their approved Statement of Work (SOW)."[268] The Marines, while having military analysts, have relied heavily on contractors. However, the Marines ensure all UAS missions are conducted under military control—even COCO Scan Eagle UAS missions are directed by a Marine OIC.[269] The Navy relies heavily on contractors for aircraft and sensor operations for its smaller number of UAS missions, but has utilized military intelligence analysis officers exclusively on these missions.[270]

According to OFPP Policy Letter 11-1, Sec. 5-1:

> *A function may be appropriately performed by a contractor consistent with the restrictions in this section—including those involving the exercise of discretion that has the potential for influencing the authority, accountability, and responsibilities of government officials—where the contractor does not have the authority to decide on the overall course of action, but is tasked to develop options or implement a course of action, and the agency official has the ability to override the contractor's action. The fact that decisions are made, and discretion exercised, by a contractor in performing its duties under the contract is not, by itself, determinative of whether the contractor is performing an inherently governmental function.*
>
> *A function is not appropriately performed by a contractor where the contractor's involvement is or would be so extensive, or the contractor's work product so close to a final agency product, as to effectively preempt the Federal officials' decision-making process, discretion or authority.*[271]

Accordingly, it would be reasonable for the workforce to remain heavily dominated by government personnel. Likewise, it would be reasonable for government employees not to be so junior and inexperienced that they would tend to seek leadership from a more experienced contractor workforce—the military member cannot be a rubber stamp for contractor decisions.

---

[266] Cloud, *Civilian Contractors, supra* note 1.

[267] Ryan Email, *supra* note 247.

[268] *Id*.

[269] *Id.*

[270] NAVAIR *Fire Scout, supra* note 264.

[271] OFPP Policy Letter 11-1, *supra* note 128, at 5-1(a)(ii)(A) & 5-1(a)(ii)(B).

The recent Air Force investigation of an erroneous drone strike in the Uruzgan Province, central Afghanistan, raised questions concerning the possibility of inappropriate use of contractors for tactical intelligence and target identification. In February 2010, Hellfire missiles, launched from an Air Force Predator, killed 15 Afghan civilians, and injured at least a dozen more, travelling in a three vehicle convoy near U.S. special operations forces who were conducting a capture mission. Investigations into the miscalculated decision to strike revealed that although the Predator was piloted and operated by military personnel, and the decision to fire was made by the ground force commander, the decision was largely based upon intelligence analysis conducted and reported by a civilian contractor.[272] Arguably, this reported contractor activity should not be viewed as inherently governmental since it did not involve "direction and control of intelligence" or final decision making, but it should at least be considered very closely associated with inherently governmental activities, namely, the decision to strike—to engage in offensive combat. Some authorities, however, contend that contractor production of tactical intelligence products closely correlated to kinetic weapons targeting decisions not only exceeds Defense Department and OFPP limitations on inherently governmental functions, but also potentially violates international laws of war.[273]

Current DoD initiatives ensure that military personnel dominate UAS tactical intelligence activities and strengthen the armed forces' ability to prevent future inappropriate—arguably, unlawful—contractor involvement. By assigning the majority of analysis functions to military personnel, and by placing ultimate command and decision authority with more senior military officers, the DoD is developing UAS intelligence analysis capabilities in a manner that complies with applicable Inherently Governmental Function policy and guidance. Nevertheless, the military services should be vigilant to avoid contracted intelligence activities where civilians may exert a significant amount of influence or control over targeting and weapons release decisions. It is imperative that Defense Department contractors not get too close to the tip of the spear. Although intelligence analysis, per se, is not inherently governmental, it is susceptible to being closely associated with inherently governmental combat functions, and should therefore be under the control of military decision making authorities.

4. Aircraft, Sensor and Weapons Operations

(a) *Medium and Large UAS*

---

[272] Supra note 1.

[273] *See generally* Duane Thompson, *Civilians in the Air Force Distributed Common Ground System (DCGS)*, Joint Center for Operational Analysis J., June 2008, at 23–24 (stating that the Air Force Operations Law Division has concluded that intelligence personnel delivering "tactical intelligence relevant to targeting for real-time missions that inflict harm to enemy personnel and property" should be military members because the individuals are performing "targeteer" functions—that is, "[p]ersons who relay target identification for an imminent real-world mission to persons causing actual harm to enemy personnel or equipment").

OFPP Letter 11-1 and DODI 1100.22 both proffer a fairly simple idea: "combat" and "direction and control of intelligence" operations are inherently governmental. According to the Pentagon's RPA Capabilities Division, only Air Force pilots currently fly Air Force planes, be it an F-16 Falcon, A-10 Warthog, MQ-1 Predator, or any other fixed or rotary wing aircraft.[274] According to Lt Col Bruce Black of the RPA Task Force, only Air Force pilots have flown planes, but soon a new type of military officer will be flying UAVs.[275] According to Charles Blanchard, "[i]n the Air Force system right now, the launch and recovery folks are all military. The folks piloting and [performing] weapons operations are all military."[276] In short, when it comes to the medium and large UAS missions (i.e., MQ-1 Predator, MQ-9 Reaper, and RQ-4 Global Hawk), the Air Force has embraced a pretty simple policy: the operation of a combat aircraft—whether flown for targeted strikes or intelligence gathering—is an inherently governmental function that should be performed by federal personnel, or more specifically, military officers.[277]

At this time the Army operates three medium class UAS: the MQ-5B Hunter, MQ-1C Gray Eagle, and the Warrior Alpha. As previously discussed, the 2,000 pound Hunter is a tactical ISR vehicle capable of delivering anti-tank munitions;[278] and the Gray Eagle is a next generation Predator variant, outfitted with advanced sensors and capable of delivering four Hellfire missiles.[279] Although the Army has developed a robust UAV operations training program for the last several years, both military personnel and contractors have operated the Hunter and the Gray Eagle's predecessor, the MQ-1C Warrior, while deployed to a theater of operations.[280] The Army initially fielded the Warrior Alpha as a quick reaction capability asset in 2004 to support both Operations Enduring Freedom and Iraqi Freedom.[281] Teams of private contractors deployed to both Iraq and Afghanistan

---

[274] Lt Col Recker Interview, *supra* note 68.

[275] *The Future of Unmanned Air Power, supra* note 67. (referring to the 18X career field, in which officers will receive pilot training that removes much of the training elements necessary to prepare pilots for traditional manned military aircraft, e.g., SERE (survival, evasion, resistance, escape) training).

[276] *Drones Promise, supra* note 255.

[277] The Air Force's current position on UAS operation has become more conservative over the last few years. For example, *see* Air Force Strategic Vision, *supra* note 206.

[278] Gertler, *supra* note 42, at 42; Army Roadmap, *supra* note 45, at 77.

[279] GAO-09-520, *supra* note 31, at 16-18.

[280] Bill Sweetman & Paul McLeary, *Some UAV Makers Do Better Than Others*, Aviation Week, Sep.10, 2009, *available at* http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/UAVs091009.xml&headline=Some%20UAV%20Makers%20Do%20Better%20Than%20Others (quoting Colonel Greg Gonzales, Army Project Manager for Unmanned Aircraft Systems, who says that most RQ-5 Hunters and MQ-1C Warriors are flown by contractors); Army Roadmap, *supra* note 45, at 45 (briefly discussing a GOCO Hunter unit that deployed in support of Operation Iraqi Freedom in September 2006).

[281] Anthony S. Pelczynski, Rapid Acquisition Impact on Major Defense Acquisition Programs, U.S. Army War College Paper submitted in partial fulfillment of degree requirements, Mar. 30, 2010, at 18, *available at* http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA520036.

to support the Government-Owned, Contractor-Operated (GOCO) system, which was tasked to support Task Force Observe, Detect, Identify, and Neutralize (TF ODIN) intelligence collection requirements.[282] The technology immediately produced positive impacts—in 2006 alone, TF ODIN found and killed over 2400 insurgents, and captured 141.[283] The Warrior Alpha continues to support TF ODIN Afghanistan operations, with contractors performing launch and recovery activities, and augmenting sensor and aircraft operations as needed.[284]

According to the Army's Unmanned Aviation Operations, Plans, and Training Branch, contractors often operate unmanned aircraft, but the military is in control of the mission.[285] Contractors do not operate UAVs that are armed and capable of dropping weapons, capable of engaging a target with a laser targeting system, or able to conduct electronic warfare.[286] If flying, contractors are conducting missions limited to ISR or assisting launch and recovery.[287] While contractor operators do not "get to fire weapons or laze targets, contractors can feed data to ground troops."[288]

The Navy currently employs one large UAS, the Broad Area Maritime Surveillance (BAMS) System, and one medium class vehicle, the MQ-8B Fire Scout, the Navy's unmanned helicopter. The Marines do not field a medium or large class UAV. Of the five BAMS procured by the Navy, two are operational but the Navy only fields one at a time in theater, where it is currently flown by U.S. Navy P-3 and P-8 rated military pilots.[289] As of December 29, 2011, three Fire Scout expeditionary units are currently conducting ISR missions in Afghanistan; as expeditionary units, they are forward deployed to a ground station rather than operate from a Naval vessel.[290] All of the Fire Scout operators at this time are contractors—"this is a GOCO Fire Scout mission."[291] The Navy has not armed the Fire Scout at this time,

---

[282] *Id*., at 21; Singer, *supra* note 58, at 223; Lt Col Cutting Interview, *supra* note 52.

[283] Singer, *supra* note 58, at 223.

[284] Lt Col Cutting Interview, *supra* note 52 (Because the Warrior Alpha did not evolve into an actual development program, but was replaced by the Gray Eagle, the Army has continued to rely heavily on the contractor for sustainment and operation since no Soldiers were to be trained for future support of the Warrior Alpha).

[285] *Id*.; Ryan Email, *supra* note 247.

[286] *Id.*

[287] *Id.*

[288] *Id.*

[289] Interview of D. Jeff Hurley, CAPT, U.S. Navy (retired), former Branch Chief, Navy Unmanned Air Capabilities (OPNAV N2/N6), Dec. 29, 2011 [hereinafter Hurley Interview] (stating that of the two operational BAMS, one is almost always forward deployed with the 5th Fleet, and one is back at the Patuxent River Test and Evaluation Facility for repair, modification, and further evaluation) Interview notes on file with author. Mr. Hurley can be contacted online at http://www.linkedin.com/pub/jeff-hurley/19/860/2a9.

[290] *Id.* (The Fire Scout was originally planned to operate from the Navy's new Littoral Ships still in development. Because the littoral ships are not presently available, the Navy has decided to use the Fire Scouts from a traditional land based operation.); *see also* NAVAIR *Fire Scout, supra* note 264.

[291] Hurley Interview, *supra* note 289.

but will arm the vehicle in the near future.[292] The Fire Scout, however, is equipped with "full motion video and imagery from its electro-optical and infrared sensor[s]" and uses lasers to designate "targets for troops in the field."[293]

(b) *Small Tactical UAS*

All of the services have relied heavily upon contractors for the operation of small tactical UAS. These small aircraft are remotely piloted by individuals on the ground, who are in receipt of direct camera feeds. "Small UAVs provide a unique capability to get close to a target and provide the 'bird's eye view.' Their small size, quiet propulsion systems, and ability to feed information directly" to troops on the ground enhances the combat effectiveness of military forces.[294] For the Air Force, the SUAS mission appears to be the only Air Force unmanned mission that existed recently (and may still exist) where military members are not always in operational control. The Air Force currently employs three types of small tactical UAS: the RQ-11B Raven, the Wasp III, and the Scan Eagle.[295] Although the Air Force owns these aircraft, which are utilized by troops in theater, these UAS have been operated by contractor personnel.[296] The Army employs a number of small UAS, including the RQ-7 Shadow, RQ-11 Raven, gMAV/T-Hawk, and Switchblade.[297] Unarmed—excepting the Switchblade—these SUAS provide immediate ISR capabilities to ground forces, and are operated by both military and contractors.[298] The Navy and Marines have likewise procured and employed the Shadow, Raven, and gMAV/T-Hawk SUAS, but also utilize the manufacturer Insitu's contractor-owned, contractor-operated (COCO) Scan Eagle UAV services.[299] While these Navy and Marine SUAS are currently unarmed, the Marines are presently developing an armed version of the Shadow.[300]

(c) *Contractors Connected to the Kill Chain and Inherently Governmental Functions.*

The more closely related an activity is to the kill chain, the greater the likelihood the activity should be barred from contractor performance. Without

---

[292] *Id.*

[293] NAVAIR *Fire Scout, supra* note 264.

[294] Air Force Strategic Vision, *supra* note 206, at 5.

[295] *Supra* note 53.

[296] GAO-09-175, *supra* note 57, at 7.

[297] Gertler, *supra* note 34, at 8; Beidel, *supra* note 49; *Popular Science, supra* note 49.

[298] Ryan Email, *supra* note 247 (describing RQ-7B Shadow contractor support: "During the current conflict the Army asked the Vender [sic.] to build several detachments of Shadow System to augment currently deployed forces. These detachments are placed under the control of other Army Shadow Units to assist with C2 and tasking").

[299] GAO-09-175, *supra* note 57, at 7.

[300] Lt Col Cutting Interview, *supra* note 52.

doubt, an individual who pilots an armed UAV in support of an overseas contingency operation, and who releases a weapon at an identified enemy target, is engaging in combat. Such action is recognized as inherently governmental and may only be performed by government employees, or more specifically, may be only performed by lawful combatants, meaning military personnel.[301] The same should be said for operating a laser targeting system from a UAV. By "painting" or "lazing" a target so American forces can more accurately direct fire against the enemy, a laser designator operator is directly participating in the intentional infliction of violence.[302] Although the Army has stated contractors are not allowed to operate UAVs capable of lazing targets, the Navy GOCO Fire Scout, which is currently deployed to Afghanistan, possesses and utilizes this targeting capability.[303] But, what should be said about the operation of sensors to gather information, images, and video? As the former head of the Navy Unmanned Air Capabilities Branch put it, "[i]f [the sensor operators] are just drilling holes in the sky, do they have to be in the military?"[304] For many commentators, the question hinges on whether the intelligence being collected is for the formation of strategy or for conducting tactical operations.[305]

The primary missions of UAS are (1) to provide reconnaissance, "using sensors to detect and observe objects on land or sea or to intercept and analyze electronic emissions from ground, sea, or air sources; and (2) to provide "light attack" capability.[306] Because of these capabilities, the military branches all recognize the value UAS hold as "sentries," monitoring surroundings and potentially striking or assisting with targeting as needed.[307] Indeed, UAS technology has the ability to feed data to troops to plan force protection and special operations missions, or possibly to provide direct strike capability. This ability describes the technology as capable of combat operations, or very closely associated with the inherently governmental function of combat. Because of such combat capability and/or associations, the role of an UAS contractor operator is analogous to the role of a private security contractor.

---

[301] Protocol I, *supra* note 175, art. 43(2). *See also* DoDI 1100.22, *supra* note 143, at Enclosure 4, ¶1.c.(2); Davis, *supra* note 29; Johnson, *supra* note 29.

[302] ICRC, DPH Guidance, *supra* note 253, at 47 ("For a specific act to qualify as direct participation in hostilities, the harm likely to result from it must attain a certain threshold. This threshold can be reached either by causing harm of a specifically military nature or by inflicting death, injury, or destruction on persons or objects protected against direct attack. The qualification of an act as direct participation does not require the materialization of harm reaching the threshold but merely the objective likelihood that the act will result in such harm. Therefore, the relevant threshold determination must be based on "likely" harm, that is to say, harm which may reasonably be expected to result from an act in the prevailing circumstances." *Citations omitted*).

[303] Ryan Email, *supra* note 247; Hurley Interview, *supra* note 289.

[304] Hurley Interview, *supra* note 289.

[305] *Supra* note 163 ("Strategic intelligence" defined); *supra* note 164 ("Tactical intelligence" defined); *see also supra* note 253 (Discussion of tactical intelligence constituting direct participation in hostilities).

[306] CBO Policy Options, *supra* note 35, at 28.

[307] *Id*.

Formed in 2008, the Commission on Wartime Contracting in Iraq and Afghanistan (CWC) conducted a multi-year assessment of contingency contracting for reconstruction, logistics, and security functions. In addition to identifying at least $30 to $60 billion lost to fraud and waste, the CWC concluded that existing law and policy on inherently governmental functions did not effectively guide contracting officers and commanders on the appropriate use of contractors.[308] According to the CWC, this lack of effective guidance, coupled with military manpower shortages and preferences for privatization, led the U.S. Government to contract for services that should have remained under the control of government personnel.[309] Focusing heavily on the use of private security contractors in Iraq and Afghanistan, who had been engaged in hostile fire incidents on several occasions, the CWC made four recommendations to Congress regarding inherently governmental function policy and law: (1) use risk factors in deciding whether to contract in contingencies, (2) develop deployable cadres for acquisition management and contractor oversight, (3) phase out use of private security contractors (PSCs) for certain functions, and (4) improve interagency coordination and guidance for using security contractors in contingency operations.[310]

OFPP incorporated many of the key CWC recommendations into Policy Letter 11-1. For example, in addition to providing more detailed guidance for defining inherently governmental functions, and creating the categories of closely associated and critical functions, the policy letter attempts to identify the security activities that are at risk of becoming inherently governmental. While OFPP recognizes that contractors are entitled to act in self-defense or in defense of others, the policy letter identifies three circumstances where security operations are inherently governmental:

> *(a) Security operations performed in direct support of combat as part of a larger integrated armed force.*
>
> *(b) Security operations performed in environments where, in the judgment of the responsible Federal official, there is significant potential for the security operations to evolve into combat. Where the U.S. military is present, the judgment of the military commander should be sought regarding the potential for the operations to evolve into combat.*
>
> *(c) Security that entails augmenting or reinforcing others (whether private security contractors, civilians, or military units) that have become engaged in combat.*[311]

---

[308] *See generally* CWC Final Report, *supra* note 2.

[309] *Id.*

[310] *Id.* at 49, 52, 61 and 64.

[311] OFPP Policy Letter 11-1, *supra* note 128, at Appendix A, 5(a)-5(c).

It follows that when an operator remotely pilots a drone to an area for the purpose of engaging an adversary using UAV delivered munitions, collecting intelligence that will be delivered to combat forces currently engaged in hostilities, or gathering and delivering intelligence data to troops facing circumstances with "significant potential…to evolve into combat"—the UAV operator's activities mirror the security activities described above. UAS operations involve a foreseeable likelihood that intelligence or reconnaissance missions could quickly erupt into combat operations. As such, because the principle military operations of small tactical UAVs are intelligence or reconnaissance, UAV operations would be regarded as inherently governmental and prohibit mission performance by contractor personnel.

(d) *Limiting Contractor Involvement in the Kill Chain*

Is a UAS pilot or sensor operator outside the kill chain if the operator is not dropping bombs or launching missiles? As previously mentioned, there are basically six steps in the kill chain—find, fix, track, target, engage, and assess (F2T2EA).[312] Providing tactical intelligence directly to ground troops to help them locate, track and engage enemy forces is clearly within the kill chain—without good intelligence, the commander is operating at a huge disadvantage. With an eye in the sky reporting directly what is around the corner or over the next hill, the commander is better able to successfully execute attacks as well as protect the troops in contact with enemy forces. Additionally, while precise targeting is regarded as an important, humane, objective, it is still direct support of combat activities. Similarly, using lasers to designate targets for strikes by manned aircraft or artillery is often the critical penultimate step before an attack. Precise targeting increases mission effectiveness, and minimizes civilian injury and death. An overly constricted view of the kill chain would ignore the close connection UAV pilots, sensor operators, and laser designators can have to a combat role. Although the laser guided missile may be launched from another location, the laser emission or data coming from the UAV is often the key component to ensuring the missile strikes what the ground force commander needs to be taken out.

To adhere to current policy and law regarding the performance of inherently governmental activities, one practice that DoD can adopt is to only allow military personnel to serve as aircraft pilots and UAS sensor operators. Put simply, functions like piloting aircraft and operating UAS sensors are so intimately related to the public interest they require performance by Federal Government employees. Included among these functions are activities that significantly affect the life, liberty or property of private persons,[313] such as military combat operations. Combat operations by the U. S.Armed Forces are exercises of federal sovereign authority that undeniably

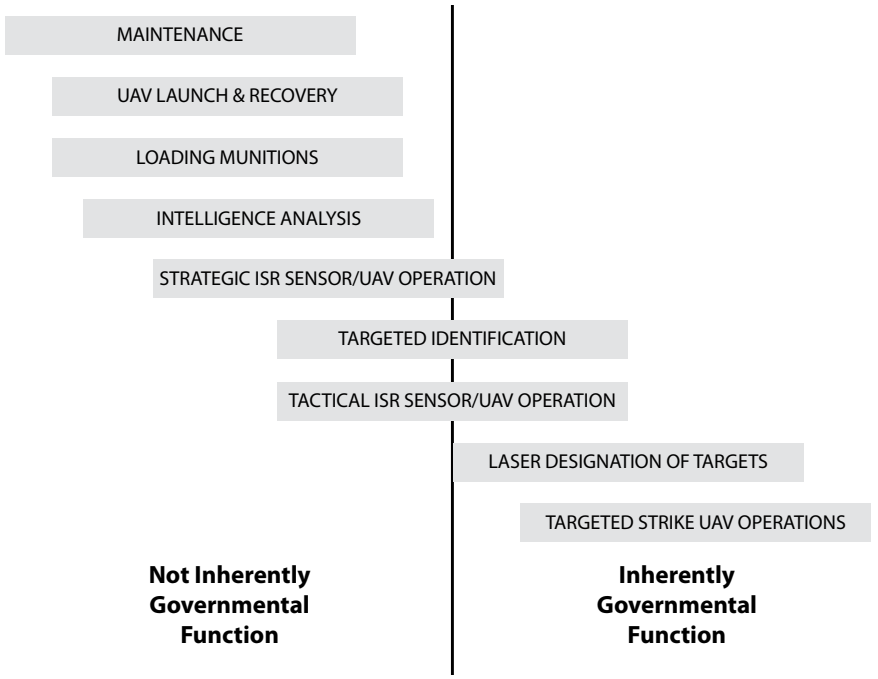
[312] *See supra* notes 209-11.

[313] *See generally* OMB Circular A-76, *supra* note 97, at Attachment A, ¶B.1.a.3; 31 U.S.C. § 501 note, *supra* note 107, at § 5(2)(B)(iii); OFPP Policy Letter 11-1, *supra* note 127, at §3(a)(3); DoDI 1100.22, *supra* note 144, at Enclosure 4, ¶1.c.

affect the lives, liberty interests, and property of private persons.[314] Under the policy and law described above, the practice of using contractor operated UAS in theater for tactical intelligence collection and dissemination, precision laser targeting, or kinetic force delivery can be described as combat operations. Accordingly, under current OFPP policy, DoD Instructions, and Federal law, practices should be avoided that use contractors to perform functions recognized as combat operations, or that have the foreseeable likelihood of evolving into combat operations.

V. KEEPING CONTRACTORS FROM CROSSING THE LINE: PROPOSED ACTIONS

Despite manpower limitations and overwhelming pressure to conduct continuous UAS operations throughout the Middle East and Southwest Asia, the U.S. military has been tremendously successful in keeping civilian contractors from performing roles that would be clearly governmental. However, UAS activities present a range of functions in which contractor performance needs to avoid crossing the line for inherently governmental functions. Accordingly, the contractor functions in these activities need to be carefully evaluated in both their planning and execution. Figure 3 presents general categories of UAS mission activities in terms of the nature of each function's place on a continuum between what could be considered Not Inherently Governmental and Inherently Governmental.



[314] Compare, for example, Verkuil, *Outsourcing and the Duty to Govern, supra* note 105, at 326 (arguing that "the use of private military contractors such as Blackwater" violated inherently governmental activity restrictions because the contractors' actions significantly affected the life, liberty or property of private persons.)

Figure 3: Categorizing the Governmental Nature of UAS Activities

Figure 3 illustrates functions that are nongovernmental, and illustrates functions (e.g., piloting or firing missiles on targeted strike missions) that are inherently governmental. Figure 3 also illustrates functions that are at risk of crossing the line of inherently governmental functions. The Figure further illustrates how certain functions (e.g., Tactical Sensor/UAV Operation) are at greater risk of crossing the line for inherently governmental functions due to those functions' close correlation to combat. Consistent with the above analysis in Section IV, these functions should be designated for performance by government personnel—specifically, military personnel in active duty status.

The U.S. military's principal activities in maintenance, intelligence, and operation of medium and large UAS reportedly adhere to the guidance espoused in OFPP Policy Letter 11-1 and DoDI 1100.22.[315] However, contractor operated UAS are at greater risk of improper performance of an inherently governmental function. For example, there have been situations where contractors have played important roles in the processing of intelligence that ultimately led to decisions to initiate air strikes. Moreover, enforcement of prohibitions against improper contractor activity is somewhat problematic. At this time, contractors do not have truly effective civil liability remedies for challenging agency decisions to use contractors for UAS missions.[316] Additionally, it is uncertain whether tort actions could be used successfully against individual contractors or private companies alleged to have committed misconduct while performing UAS mission tasks, or whether contractors performing the same work as government team members would be equally shielded from liability.[317]

---

[315] Although, as previously noted throughout Part IV: Analysis of Current UAS Functions and Roles of Contractors, situations have occurred in which contractors have possibly performed, or risked performance of, inherently governmental functions. *See also supra* notes 1, 57, 68.

[316] For a good discussion of the problems with challenging whether a function should be considered inherently governmental, please see the Brian X. Scott case history: *Brian X. Scott*, Comp. Gen. B-298370, 2006 WL 2390513 (Aug. 18, 2006) (denying protest that alleged Defense Department solicitations for contracts to transport cargo in Iraq contracted out inherently governmental functions by calling for armed security escorts; GAO concluded that existing laws and regulations permitted contracts for armed security when contracts prohibited contractors from performing offensive or combat operations); *Bryan X. Scott v. United States*, 78 Fed. Cl. 151 (2007) (holding that a plaintiff challenging an award of a contract must "establish that he was prejudiced by showing that he had a substantial chance of receiving the contract.").

[317] Generally, defense contractors do not enjoy the same protections as federal employees who may cause harm to third parties. Unlike the government employee who is allocated defenses when performing within the scope of his work, the status of immunity afforded to a civilian contractor is unresolved, thus the contractor potentially faces third party liability even when working within what many regard as the DoD blended workforce. *See generally* Dickinson, *Outsourcing War & Peace, supra* note 4, at 52 (citing *Boyle v. United Tech. Corp.*, 487 U.S. 500, 512 (1988); *Harris v. Kellogg, Brown & Root Servs., Inc*., 618 F. Supp. 2d 400 (W.D. Penn. 2009); *Al Shimari v. CACI Premier Tech., Inc.*, 657 F. Supp. 2d 700 (E.D. Va 2009)).

Compare, however, recent cases where the doctrine of sovereign immunity was expanded, affording protections to private contractors. *See e.g. Saleh v. Titan Corporation & CACI International Inc.*,

Scholars have commented that contractors involved with UAS and other battlefield operations might be subject to prosecutions in foreign courts or in International Criminal Court.[318] These commentators raise the question of whether contractors travelling outside the U.S. might be at risk of being arrested and charged for misconduct in performing their contracts. And, while the U.S. enacted the Military Extraterritorial Jurisdiction Act (MEJA) and broadened the authority of the Uniform Code of Military Justice (UCMJ) to enable the prosecution of Defense contractors for serious crimes committed abroad, research to date was unable to discover any data that would indicate these statutes have ever been seriously considered in order to prosecute contractors for alleged war crimes or other felonies (if any) that might arise from UAS operations.[319] In fact, most federal circuit cases concerning UAS missions do not address U.S. operations. Instead, ancillary issues were raised, such as the effect of Base Realignment and Closure (BRAC) efforts,[320] contract payment

580 F.3d 1, 388 U.S. App. D.C. 114 (2009) (Victims from Abu Ghraib barred from relief from contractors who participated in detainee abuse on grounds that contractor who is "fully integrated into military units" is preempted from lawsuit); *McMahon v. Presidential Airways*, 502 F.3d 1331 (2007) (court appears to create a "military judgment" immunity, that said if contractor has decision making capability, then could possibly get immunity).

[318] *See e.g.,* Turner & Norton, *supra* note 187, at 32, 69-70 (describing unlawful combatants' loss of POW status and the possibility of prosecution for war crimes by the International Criminal Court (ICC) or "under the law of the Detaining Power"); Vernon, *supra* note 170, at 417 ("Parties may prosecute as war criminals those contractor employees taking a direct part in hostilities. Acts of hostility committed by private individuals are punishable as war crimes, not because those actions are contrary to the law of armed conflict, but because it is unlawful for private individuals to wage war"); Schmitt, *War, supra* note 196, at 519-21 (Stating that civilians who directly participate in hostilities may be targeted and could be punished/prosecuted for their actions; unprivileged belligerents lose all combatant immunity); Blizzard, *supra* note 192, at 11 (Describing the 2002 Rome Statute that created the International Criminal Court (ICC) ability to prosecute war crimes); Rock, *supra* note 20, at 62-3 (Stating that the United States decided not to ratify the ICC Rome Convention in part because of fear of possible contractor prosecutions); Radsen & Murphy, *supra* note 26, at 1205 (2011), citing Shane Harris, *Are Drone Strikes Murder?*, Nat'l J., Jan. 9, 2010, at 24 (discussing the possibility that "CIA employees or others involved in Predator strikes could conceivably face legal scrutiny and prosecution" by, inter alia, the International Criminal Court).

[319] Military Extraterritorial Jurisdiction Act of 2000, 18 U.S.C. §§ 3261-3267 (2000); Uniform Code of Military Justice, 10 U.S.C. §§ 801-946. It should be noted that MEJA and UCMJ's expanded jurisdiction was intended to address the misconduct of civilians physically present in the theaters of war—the question of whether MEJA or the UCMJ would apply to contractors operating from facilities back in the United States has not been tackled. For general discussions of the possibility of, and complications surrounding, the prosecution of civilian contractors, *see* Dickinson, Outsourcing War & Peace, *supra* note 4, at 49-51 & 190-92; Ian W. Baldwin, *Comrades in Arms: Using the Uniform Code of Military Justice and the Military Extraterritorial Jurisdiction Act to Prosecute Civilian-Contractor Misconduct*, 94 Iowa L. Rev. 287 (2008); Margaret Prystowsky, *The Constitutionality of Court-Martialing Civilian Contractors in Iraq*, 7 Cardozo Pub. L. Pol'y & Ethics J. 45 (2009). *See also United States v. Slough*, 641 F. 3d. 544 (2011) (illustrates the difficulties of determining the correct jurisdiction for the prosecution of serious criminal offenses committed against local nationals in a theater of war, and the difficulty of preserving evidence necessary for prosecution).

[320] *See e.g. Blagojevich v. Gates*, 558 F.Supp.2d 885 (2008); *Bresdesen v. Rumsfeld*, 2005 WL 2175175 (M.D.Tenn. 2005); *Rell v. Rumsfeld*, 389 F. Supp. 2d 395 (2005) (Each case representing concerns raised about pending closures of Air Force and Air National Guard Bases, where UAS squadrons and other flying units operated).

claims,[321] patent infringement actions,[322] or illegal arms exports.[323] Moreover, in the few instances where the issue of U.S. Government unmanned targeted strike operations has been brought before Federal judges, the courts have ruled that agency records of drone operations are protected from public disclosure by Freedom of Information Act (FOIA) exemptions,[324] and have indicated that judicial rulings on the legality of UAS strikes may be inappropriate for the courts.[325]

Under the foregoing analysis, the prospects for civil remedy and Federal criminal jurisdiction are nebulous. Moreover, potential protection from the risks contractors may face in foreign courts is similarly nebulous. In response, the remedy is to avoid contractors crossing the line of inherently governmental functions. The following actions are proposed to support this remedy:

---

[321] *See e.g. Parker v. Donley*, 379 Fed.Appx. 980, 2010 WL 2330408 (C.A.Fed. 2010), *rehearing denied* (United States Court of Appeals for the Federal Circuit held that an invoice submitted by a contractor who produced Predator training software did not constitute a proper claim under the Contract Disputes Act (CDA)).

[322] *See e.g. Gal-Or v. United States*, 93 Fed.Cl. 200 (2010) (The plaintiff, a foreign patent applicant, filed *pro se* against the United States, alleging a variety of claims regarding intellectual property rights related to manned and unmanned aircraft. The United States Court of Federal Claims granted the government's motion to dismiss for failure to state a claim).

[323] *See e.g. United States v. Hanson*, 613 F. Supp. 2d 85, 87 (2009) (Bond review for one of two defendants charged with conspiracy to violate and for violations of "the International Emergency Economic Powers Act, 50 U.S.C. § 1705, and the Export Administration Regulations, 15 C.F.R. §§ 744 and 764.2. . . The indictment alleges that the defendants illegally exported unmanned aerial vehicle ("UAV") autopilot components to the People's Republic of China."); *United States v. Bout,* 2011 WL 2693720 (S.D.N.Y. 2011) (Denial of Defendant's motion to dismiss Indictment, in which is charged conspiracy to provide the FARC [a known Columbian terrorist organization] with millions of dollars' worth of weapons [including unmanned aerial vehicles] to be used (i) to kill U.S. nationals, officers, and employees, (ii) to protect FARC cocaine trafficking, and (iii) to attack U.S. interests in Columbia.)

[324] *American Civil Liberties Union v. Department of Justice*, 808 F.Supp.2d 280 (2011) (The ACLU brought a FOIA action against the Central Intelligence Agency (CIA) and other Federal agencies seeking records documenting the "alleged practice of using unmanned drones to kill selected human targets." The U.S. District Court, District of Columbia, granted the Government's motion to dismiss on grounds that "(1) existence of relevant records fell within FOIA exemption for materials exempted from disclosure by non-FOIA statutes; (2) CIA did not officially acknowledge practice or records, and thus did not waive its ability to deny existence of records; and (3) existence of relevant records fell within FOIA exemption for information subject to executive order to be kept secret in interest of national defense or foreign policy.").

[325] *Albihani v. Obama*, 619 F.3d 1, 40-41, 393 U.S.App.D.C. 57, 96-97 (2010) (The Court denied the Guantanamo detainee's Petition for Rehearing *En Banc* to determine the role of international law-of-war principles in interpreting the 2001 Authorization for Use of Military Force(AUMF). In a concurring opinion providing a lengthy analysis, Judge Kavanaugh argued that international norms outside of those expressly incorporated into U.S. domestic law by the political branches were not enforceable by federal courts after the Supreme Court's 1938 decision in *Erie Railroad Co. v. Tompkins*, 304 U.S. 64, 58 S.Ct. 817, 82 L.Ed. 1188 (1938). Using the question of the legality of drone strikes as an illustration, Kavanaugh opined that "judicial assessment of contested international-law norms" and imposition of limitations on Presidential warfighting powers would be an inappropriate interference with "the President's duty and responsibility to win the war, in a manner consistent with the Constitution and with constitutionally permissible limits imposed by Congress.")

(1) Defense acquisition professionals rigorously apply the principles of OFPP Policy Letter 11-1 and DoDI 1100.22 to UAS systems and support procurement human capital requirements planning.

(2) Congress and the DoD establish appropriate transparency and accreditation regimes.

(3) Congress provide the military with the manning and training budgets needed to develop a skilled cadre of federal employees (principally military personnel) to fulfill the majority of roles within the UAS mission.

(4) Congress strengthen the Defense Acquisition Workforce to ensure proper management of critical contractor personnel.

A. Procurement Planning for UAS Human Capital Requirements

As described in this Article, the DoD UAS requirements vary greatly for each military branch. Accordingly, each military branch has service-specific requirements for avoiding crossing the line for inherently governmental functions. For each military branch to retain control over its UAS human capital requirements planning, each military branch must ensure that potential inherently governmental activities are identified in the early stages of procurement planning. Importantly, each military branch needs to take the steps to avoid the inappropriate contracting of jobs that should be performed by the government. Failure to do so could result in Congress denying the DoD the discretion to decide for itself what UAS roles may be performed by contractors.

As previously mentioned, OFPP drafted Policy Letter 11-1 in response to directions given to OMB by the President to clarify "when governmental outsourcing for services is and is not appropriate."[326] The policy letter, however, was a product also arising from the authority granted by "section 6(a) of the Office of Federal Procurement Policy Act, 41 U.S.C. 405(a) . . . and section 321 of the Duncan Hunter National Defense Authorization Act for Fiscal Year 2009, Public Law 110–417."[327] Both the President and Congress recognized that reliance on private contractors had become overwhelming, and the Government needed to slow its outsourcing efforts and develop a better understanding of what work was best retained by the government. As noted in the House report on the 2009 NDAA, the task of deciding which functions must be performed by government employees "is made even more

[326] *Supra* note 127.

[327] OFPP Policy Letter 11-1, *supra* note 128, at 56236, ¶2.

difficult by the lack of a single definition and accompanying guidance on what constitutes an 'inherently governmental function.'"[328]

In 2009, the Senate introduced legislation intended to "diminish agencies' ability to contract out inherently governmental functions."[329] Through the Correction of Long-Standing Errors in Agencies' Unsustainable Procurements (CLEAN-UP) Act of 2009 (S. 924, 111th Congress), Congress intended to "adopt the FAR's definition of functions closely associated with inherently governmental functions," create definitions of mission essential functions, define "other categories of functions related to inherently governmental ones" and preclude agencies from contracting those functions."[330] The Senate Bill and the identical House Bill, H.R. 2736 were both referred to committee, where they were read but no further action was taken.[331] Successor proposals consistent with the CLEAN-UP Act proposal, however, may ultimately place statutory restrictions on inherently governmental functions. For example, in May 2011, both the House and Senate introduced the proposed legislation again, which is now in committee.[332] If passed, the law would force agencies to identify improper dependence on contractors and to take proactive steps to return improperly outsourced work to federal employees.[333]

Both OFPP Policy Letter 11-1 and DoDI 1100.22 provide helpful guidance for all military branches in making informed, well-reasoned outsourcing decisions. This guidance provides valuable tools for assessing whether a UAS mission activity should be considered (1) work the government must perform in-house because it is inherently governmental, (2) work the government should perform in house because it is closely related to inherently governmental work or for other policy reasons, or (3) work that can be contracted out to the private sector. This guidance can be useful in avoiding the bad contract planning that results in bad contracts. Importantly, before contracting UAS activities to the private sector, the DoD acquisition personnel, under this guidance, would clearly identify the tasks that individual contractors are to perform. If UAS activities are appropriate for contracting, the Statement of Work should be drafted in a manner that delineates authorized activities from tasks that are, or risk becoming, inherently governmental. For functions that are at risk of

---

[328] Luckey, *supra* note 78, at 26 (citing Duncan Hunter National Defense Authorization Act for Fiscal Year 2009: Report of the Committee on Armed Services of the House of Representatives on H.R. 5658 Together with Additional Views, 110th Cong., 2d Sess. 333-34 (2008)).

[329] *Id.*, at 28 (citing Correction of Long-Standing Errors in Agencies' Unsustainable Procurements (CLEAN-UP) Act of 2009, S. 924, 111th Cong, §2).

[330] *Id.*

[331] Library of Congress, Bill Summary and Status, 111th Congress (2009 - 2010), Correction of Long-Standing Errors in Agencies' Unsustainable Procurements (CLEAN-UP) Act, S.924, *available at* http://thomas.loc.gov/cgi-bin/bdquery/z?d111:SN00924:@@@L&summ2=m&.

[332] The history of 112th Congress action on H.R. 1949 and S.991 can be found at Library of Congress, Bill Summary and Status, 112th Congress (2011 - 2012), H.R.1949, *available at* http://thomas.loc.gov/cgi-bin/bdquery/z?d112:HR01949.

[333] *Id.*

crossing the inherently governmental line as established by OFPP 11-1 and DoDI 1100.22—e.g., activities closely tied to combat, or likely to cause severe injury or loss of life—then acquisition professionals need to initiate a Determinations and Findings (D&F) process through which senior leaders decide on the appropriateness of a contract's proposed scope of work. Such a robust system of initial planning and senior level review preserves DoD's control over human capital requirements planning for UAS missions and addresses many Congressional concerns over improper contracting.

B. Creating Transparency and Accreditation Regimes

Trying to establish transparency and accreditation within the UAS community is susceptible to conflict. While openness and accountability to the U.S. taxpayers is needed, national security often demands limits.[334] Surprisingly, the military branches have been remarkably open about their UAS missions. All services provide printed and on-line information about the aircraft and capabilities. For example, on the Air Force's official web site, anyone can download facts sheets about all unmanned vehicles in the inventory, with details on technical specifications, photographs, missions, and often basing arrangements.[335] Regularly, senior leaders and subject matter experts provide lectures and presentations before industry, academic, and advocacy groups regarding present and future mission capabilities.[336] Further, acquisition planning and contract information is available on several widely known web sites.[337] However, the military understandably declines to identify individual contractors that are involved in missions, the exact roles contractors play, the details regarding the intelligence being analyzed by contractors, and the operational advice they are providing to commanders.[338] DoD accreditation

---

[334] *See generally* Laura Dickinson, Outsourcing War & Peace, *supra* note 4; Jody Freeman, *The Private Role in Public Governance*, 75 N. Y. U. L. Rev. 543 (2000); Jon D. Michaels, *Beyond Accountability: The Constitutional, Democratic, and Strategic Problems with Privatizing War,* 82 Wash. U. L. Q. 1001, (2004); Peck, *America's $320 Billion Shadow Government, supra* note 2; Michael J. Trebilcock & Edward M. Iacobucci, *Privatization and Accountability*, 116 Harv. L. Rev. 1422 (2003).

[335] *See e.g*. USAF Fact Sheets, *supra* notes 32, 37, 39, 40 & 53.

[336] *See e.g. The Future of Unmanned Air Power, supra* note 67; *Drones Promise, supra* note 255; D. Jeff Hurley, CAPT, USN (Retired), "U.S. Navy UAS Sensor Needs, Initiatives and Requirements," *Unmanned Aircraft Systems Payloads Conference*, June 19, 2012, Washington, DC, *available at* http://www.uaspayloads.net/; Lt Col James Cutting, U.S. Army, Chief, UAS Division, "Army Future Operations and Planning," *UAV Summit*, Apr. 12, 2011, Tysons Corner, VA, http://www.uavevent.com/Event.aspx?id=451032; Col Gregory Gonzalez, U.S. Army, Project Manager, Unmanned Aircraft Systems, "Striving for Unmanned Capabilities," *UAV Summit*, Apr. 12, 2011, Tysons Corner, VA, http://www.uavevent.com/Event.aspx?id=451032.

[337] CBO Policy Options, *supra* note 35; Army Roadmap, *supra* note 45; UAS Flight Plan, 2009-2047, *supra* note 231; Air Force Strategic Vision, *supra* note 206; Marine Aviation, *supra* note 231; USA Spending contract expenditures web site, *available at* http://www.usaspending.gov/; Federal Business Opportunities web site, *available at* http://www.FBO.gov/; U.S. Government Accountability Office web site, *available at* http://www.gao.gov/.

[338] Lt Col Recker Interview, *supra* note 68; Lt Col Cutting Interview, *supra* note 52; Ryan Interview,

obligations appear to be addressed through the rigorous training programs each branch has established or is currently developing.[339] While contractors continue to play important roles in the UAS mission, the DoD is aggressively stepping forward with efforts to train thousands of active duty personnel as maintainers, intelligence analysts, sensor operators, and pilots. Further, all personnel involved in UAS operations and intelligence activities—be they military, government civilian or contractor—undergo rigorous background checks in order to obtain the security clearance required by the mission.

If Congress believes current DoD efforts do not satisfy accreditation and transparency required to ensure appropriate contracting, a balance between national security and openness may be achieved through the proposed CLEAN-UP legislation described previously. Both the Senate and House versions of the bill place the exact same requirements upon agency heads—three requirements are of particular importance to Defense missions. First, agency heads must provide the OMB with annual reports on any service contracts involving new work entered into during the previous fiscal year.[340] Second, agency heads must submit to OMB a "Functions At Risk" report describing functions that should be performed solely by federal employees, but are currently being performed by contractors. For these "Functions At Risk," agencies are mandated to reduce the total number of contractor employees in such identified At-Risk functions by 70% within six years.[341] Third, agency heads are required to develop an "annual strategic human capital plan to ensure the capability" of the agency's federal employee workforce to perform agency functions.[342]

C. Developing a Cadre of UAS Personnel Within the DoD

The simplest—yet most radical and ill-advised—solution to ensuring federal performance of inherently governmental or critical UAS functions would be a congressional ban on contractor involvement in UAS missions, and the provision

---

supra note 229; Hurley Interview, *supra* note 289; Major Tidgewell Interview, *supra* note 233.

But see also Julian E. Barnes, *U.S. Rethinks Secrecy on Drone Program*, WASH. POST, May 17, 2012, *available at* http://online.wsj.com/article/SB10001424052702303879604577410481496895786.html (reporting that "[t]he Obama administration is weighing policy changes that would lift a tattered veil of secrecy from its controversial campaign of drone strikes, a recognition that the expanding program has become a regular part of U.S. global counterterrorism operations." Although the DoD "has a policy of disclosing traditional military operations once they are complete," the Pentagon has routinely declined to discuss UAS counterterrorism operations in nations other than Iraq and Afghanistan. Conversely, the CIA refuses to formerly acknowledge details of any unmanned missions. "Intelligence officials worry that if the Pentagon begins describing their operations more fully, details of the CIA's concurrent strikes could be revealed.")

[339] *See supra* Part IV.B. The Role of Contractors in the Current UAS Mission.

[340] CLEAN-UP Act, § 6, *supra* note 322.

[341] *Id*. § 7.

[342] *Id*. § 9.

of manpower allocations and training budget necessary to develop a skilled cadre of federal employees (predominantly military personnel) to fulfill the entirety of the UAS mission. Nevertheless, while more active duty forces should be allocated to the UAS mission, it is very unlikely that Congress will completely jettison contractor involvement and expertise in one of our nations' most critical wartime missions. First, the Defense Budget request for Fiscal Year 2013 demonstrates the agency's determination to reduce active duty force strength. Specifically, the DoD proposes to reduce active-duty force levels by 102,400 troops by the end of 2017, with most of the cuts applied against the Army and Marine Corps.[343] Given these proposed reductions, and the possibility that the DoD may be forced to reduce expenses further, there may not be enough active duty forces available to handle the entirety of the UAS mission. Second, eliminating all contractor involvement would be incredibly unwise. Quite often, contractors bring to a project a vast array of skills and knowledge—usually built from years of military or other government service—that proves indispensable to successful mission planning and execution. A sweeping global replacement of experienced contractors with newly minted military UAS personnel would be quite concerning. As one Air Force Lieutenant Colonel and former Predator pilot remarked: "You can't build 15 years of combat aviation experience in a year."[344]

D. Rebuilding the Defense Acquisition Workforce

Although comprehensive replacement of the contractor workforce is both unlikely and undesirable, Congress still must ensure that military UAS programs are dominated by a federal workforce in control of the mission. Moreover, in addition to forging a cadre of active duty personnel and DoD civilians ready to perform the UAS mission, Congress must allow the Defense Department to rebuild and equip its acquisition workforce with the people, resources, and skills needed to manage contractor performance within the limits described in this Article. The last several decades of Defense contracting were characterized by administrative preferences for private sector performance of many areas of government work.[345] Unfortunately, during this time where agencies increasingly turned to contractors for mission critical functions, the size of the Federal acquisition workforce was greatly reduced.[346] With agencies rendered understaffed to manage the surge of contractor personnel, it is not surprising that recent investigations into the hundreds of billions

[343] FY2013 Budget Request, *supra* note 73 at 4-13.

[344] Lt Col Recker Interview, *supra* note 68.

[345] *See generally* (OMB) Circular A-76, *supra*, note 93; Schooner, *Competitive Sourcing Policy, supra* note 93, at 270-71 (pointing out OMB Circular A-76 (2003) preference for the private sector).

[346] Steven L. Schooner & Daniel S. Greenspahn, *Too Dependent on Contractors? Minimum Standards for Responsible Governance,* J. of Cont. Mgmt., at 10, 15 (Summer 2008) (noting that from the years 1990-2006, "Congress embarked upon an ill-conceived gutting of the acquisition workforce." DoD's acquisition workforce was slashed from over 500,000 to 200,000 individuals while the procurement budget skyrocketed "from $145 billion in 1990 to over $380 billion in 2006.") (citations omitted).

of dollars spent on contract support for contingency operations arose.[347] Nor is it surprising that these investigations resulted in findings that fueled outrage over the extraordinary amount of taxpayer dollars lost to alleged contractor fraud, waste and abuse,[348] and resulted in the discovery of contractor involvement in activities that prompted worldwide rebuke.[349]

Now, as the Nation's military exits Iraq and winds down combat operations in Afghanistan, the U.S. is well positioned to commit to the rebuilding of the federal acquisition workforce.[350] Recognizing this critical need, the DoD requested $274.2 million for its Defense Acquisition Workforce Development Fund in the Fiscal Year 2013 Budget Request, an amount that more than doubled the DoD's $106 million budget for Fiscal Year 2012.[351] DoD concisely justified the requested funding as follows:

> *The FY 2013 budget supports continued strengthening of the acquisition workforce to ensure we achieve and sustain sufficient workforce capacity and capability. Since 2008, DoD has filled 6,400 new acquisition positions supported by the Defense Acquisition Workforce Development Fund. Aligned with strategy, workforce capacity has improved in critical areas such as engineering, contracting, acquisition management, and audit. Training capacity has improved by approximately 19,000 resident and 100,000 online training seats per year.* ***These improvements mitigate ongoing challenges: 17 percent of the workforce is eligible for full retirement***

---

[347] *See generally supra* note 2.

[348] *See generally supra* note 3.

[349] *See generally supra* note 4.

[350] Scholars and senior government officials have been calling for such changes for the last few years. *See generally* Schooner & Greenspahn, at 11, *supra* note 346 ("[T]oday the government needs to invest significant resources—time, money, and energy—to recruit, train, incentivize, and retain a dramatically expanded acquisition workforce.").

See also Steven L. Schooner & David J. Berteau, *Emerging Policy and Practice Issues (2010),* at 9-6, 9-8 (Dec. 1, 2010). West Gov't Cont. Year In Review Conf. Covering 2010 Conf. Briefs, Thomas Reuters, 2011; GWU Legal Studies Research Paper No. 529; GWU Law School Public Law Research Paper No. 529, *available at* SSRN: http://ssrn.com/abstract=1772824 (quoting then OFPP Administrator Dan Gordon, "The federal government has not invested in the acquisition workforce enough to allow it to adequately cope with the growth in contract spending or the increased complexity of agencies' missions …. This inattention to the workforce resulted in increased use of high-risk contracting practices and insufficient focus on contract management, as well as the especially troubling phenomenon of agency dependence on contractors to support the acquisition function." The authors later note that in 2010, Congress began "to reinvest in the acquisition workforce for the first time in two decades.").

[351] FY2013 Budget Request, *supra* note 73 at 3-11. *See also* Matthew Weigert, DoD *Wants Boost to Acquisition Workforce Fund,* Federal Computer Week, Feb. 15, 2012, *available at* http://fcw.com/articles/2012/02/15/dod-budget-acquisition-workforce-fund.aspx; Charles S. Clark, *Pentagon Seeks to Strengthen Acquisition Workforce*, Gov't Exec., Mar. 2, 2012, *available at* http://www.govexec.com/contracting/2012/03/pentagon-seeks-strengthen-acquisition-workforce/41369/.

> ***today; 19 percent are eligible within five years; workforce gains decreased 32 percent from FY 2010 to FY 2011; and losses spiked up 32 percent from FY 2010 to FY 2011.*** *In addition to completing and maintaining improved capacity, DOD will continue efforts to strengthen the quality, readiness and performance results of the acquisition workforce. The requested FY 2013 appropriation of $274.2 million for the Defense Acquisition Workforce Development Fund is critical to following through on the improvement strategy.* ***Ultimately, it is the quality of the workforce that determines the quality of our acquisition outcomes****.*[352]

More government personnel should be assigned to UAS missions, but the current state of our military indicates that (1) fewer active duty personnel will be available, and (2) the DoD will very likely continue to rely heavily on the private sector. As such, the DoD needs a body of acquisition professionals capable of managing its contracted workforce.

VI. CONCLUSION

The last decade of privatization of government activities may have reduced DoD's ability to execute its national security mission. Fighting manpower shortages and motivated to cut costs, the DoD contracted for services that should have remained under control of government personnel. As this paper has tried to demonstrate, such improper contracting potentially impacts the U. S. Armed Forces Unmanned Aircraft Systems mission. Now, while the DoD appears to have maintained government control over the most critical UAS missions, there remain a number of functions that should be reevaluated and possibly returned to federal employees to perform.[353]

Many solutions have been proposed to alleviate concern over improper, or potentially unlawful, performance of UAS roles by contractors. First, while the U.S. could always do nothing and simply hope for the best, such apathy and purposeful neglect is not an acceptable answer. The U.S. could, of course, change its current policy on Inherently Governmental Functions, and open the door to contractor personnel performing combat roles and directing intelligence operations. Such a radical change would also demand a massive, and likely unsuccessful, effort to change firmly established international laws of armed conflict.[354] It has also been suggested that the U.S. adopt "a quasi-reserve program that would require contractors

---

[352] *Id.* (emphasis added).

[353] *See* Figure 3 (identifying those UAS functions which appear to be at greater risk of involving activities that could become inherently governmental).

[354] *See* Guidry & Wills, *supra* note 205, at 13 (noting the possibility that international law could evolve to recognize a "combatant contractor legal category" but that such a change could take years); Guillory, *supra* note 182, at 136-37 (proposing the creation of a "quasi-combatant status" in International law, but recognizing the difficulty of obtaining the required multinational support).

directly participating in [UAS] operations to be reservists."[355] As recalled reservists, these contractors would serve under United States Code, Title 10 orders, subject to the military chain of command, and authorized to perform any role within the UAS mission. While such a program potentially resolves concerns discussed in this paper, implementation would demand a dramatic restructuring of the reserve programs of each branch and the development of an appropriate compensation scheme.[356]

To the extent that I previously proposed that Congress "(1) statutorily define what UAS activities may and may not be contracted" and "(2) order the development of regulations governing procurement of UAS systems and support,"[357] I do not now believe those proposals can be supported for the following reasons: Upon further investigation and reflection, and after lengthy conversation with experienced government procurement legal counsel, I see the flaws with those recommendations.[358] First, a rigid legal definition of DoD unmanned mission activities authorized for contracting will be overly constraining and also out of date as soon as it becomes law. For example, as threats and/or humanitarian concerns in the world change, the military will need flexibility in meeting human capital requirements for developing missions. That is, fixed classifications chips away at the discretion of the contracting officer and the flexibility of the military commander. Second, unmanned technology is changing rapidly, and inherently governmental function definitions in laws based upon current operations will likely fail to address next generation UAS featuring greater levels of robotics and automation.[359] Finally, because OFPP Policy Letter 11-1 and DoDI 1100.22 provide an excellent framework by which to evaluate functions, the UAS mission does not require an additional regulation to constrain procurement efforts. UAS contractors are unlike the private security contractors (PSCs) who are physically present in hostile areas, carrying firearms, involved in situations that could quickly evolve into combat-like activity, and often not under U.S. military control. Moreover, UAS contractors are typically in the United States

---

[355] Rock, *supra* note 20, at 63, citing Blizzard, *supra* note 192, at 13 ("asserting that a concept of 'sponsored reserve' serves both the function of maintaining needed military capacity while giving incentive to individuals with skills to compete for the positions"); Guidry & Wills, *supra* note 205, at 12-13 ("describing the function of the 'sponsored reserve'").

[356] *See* Blizzard, *supra* note 192, at 14 (describing the "numerous challenges that must be resolved before the Air Force can implement sponsored reserve."); Guidry & Wills, *supra* note 205, at 12-13 (stating the "development of a sponsored reserve involves a variety of issues, ranging from legal to fiscal" *citation omitted*)

[357] Keric D. Clanahan, *Drone-Sourcing? United States Air Force Unmanned Aircraft Systems, Inherently Governmental Functions, and the Role of Contractors,* 22 Fed. Cir. B. J. 135 (2012).

[358] Phone conversation with James (Ty) Hughes, former Deputy General Counsel, Acquisitions, Office of the Secretary of the Air Force (SAF/GCQ) (June 8, 2012).

[359] *See generally* Singer, *supra* note 58; Kenneth Anderson & Matthew C. Waxman, *Law and Ethics for Robot Soldiers* (Apr. 2012), Policy Review (2012 Forthcoming), *available at* SSRN: http://ssrn.com/abstract=2046375; William C. Marra & Sonia K. McNeil, *Understanding "The Loop": Autonomy, System Decision-Making, and the Next Generation of War Machines*, Lawfare Research Paper Series, No. 1-2012 (May 2012), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2043131.

or on a secured overseas base, and performing a mission controlled by a military commander. Given such differences, there is little need to impose a regulation on UAS mission commanders like the regulation recently created for PSCs.[360]

In conclusion, while contractors will continue to provide valuable expertise and support for the UAS mission, the functions outsourced to UAS contractors should not include functions that are inherently governmental, or other functions that should not be outsourced for policy reasons. Nevertheless, contracting decisions also need to evaluate risk and retain core capabilities. Accordingly, OFPP Policy Letter 11-1 and DoDI 1100.22 provide key guidance to assist all military branches in making informed, well-reasoned outsourcing decisions. As such, they also provide valuable tools for assessing the propriety of contractor activity in the UAS field. However, given the hypersonic rate of growth the DoD unmanned mission is experiencing,[361] Congress and the DoD should implement the following additional measures to protect against possible violations of the regulations and policies governing inherently governmental functions, as well as international law:

- Apply the principles of OFPP Policy Letter 11-1 and DoDI 1100.22 to UAS systems and support procurement planning.
- Pass the CLEAN-UP Act into law, and use it as a tool for UAS mission accreditation and transparency,
- Increase government manning and training for UAS missions, and
- Provide funding for further development of the Defense Acquisition Workforce.

---

[360] *See* Office of the Secretary of Defense, 32 CFR Part 159, *Private Security Contractors (PSCs) Operating in Contingency Operations, Combat Operations or Other Significantly Military Operations*, 76 Federal Register 49650 (Aug. 11, 2011) (The new regulation places a great amount of responsibility on U.S. military geographic combatant commanders, who must: "1. provide guidance and procedures for the "selection training and equipping" of PSC personnel within the commanders area of responsibility (AOR), which will address (i) registration and records maintenance for PSC personnel, (ii) training requirements verification, (iii) weapons accountability, and (iv) application procedures for firearms authorization requests; 2. ensure, through contracting offers, that PSCs understand and acknowledge contract terms and obligations; 3. identify in writing which individual PSCs are authorized to carry firearms, after case-by-case reviews by the appropriate Staff Judge Advocate, who will assess (i) where the PSC will operate, (ii) the property or persons to be protected, (iii) how movements are to be coordinated, (iv) communications plans, (v) documentation of PSC weapons and rules for the use of force training, and (vi) numerous acknowledgements by the PSC regarding criminal history, potential liability for misconduct, fitness for duty, and hostile incident reporting requirements; and ensure that "procedures, orders, directives and instructions" are available and easily accessible.")

[361] The UAS missions of all the military services have expanded greatly in the last several years, and despite current DoD budget reduction efforts, will continue to increase for the foreseeable future. Future control measures will be important for the development of appropriate force structures and weapons systems training regimes to support the totality of DoD unmanned aircraft missions. *See generally* CBO Policy Options, *supra* note 35; Integrated Roadmap, *supra* note 17; FY2013 Budget Request, *supra* note 73; Annual Aviation, *supra* note 73.

Such actions will enable the DoD to supply the appropriate human capital needed to wield this "very long, people-intensive spear" and to ensure that contractors supporting the UAS mission remain on the correct side of the inherently governmental line.

Attachment A: FAR 7.503(c)-(d) Example Functions

(c) The following is a list of examples of functions considered to be inherently governmental functions or which shall be treated as such. This list is not all inclusive:

(1) The direct conduct of criminal investigations.

(2) The control of prosecutions and performance of adjudicatory functions other than those relating to arbitration or other methods of alternative dispute resolution.

(3) The command of military forces, especially the leadership of military personnel who are members of the combat, combat support, or combat service support role.

(4) The conduct of foreign relations and the determination of foreign policy.

(5) The determination of agency policy, such as determining the content and application of regulations, among other things.

(6) The determination of Federal program priorities for budget requests.

(7) The direction and control of Federal employees.

(8) The direction and control of intelligence and counter-intelligence operations.

(9) The selection or non-selection of individuals for Federal Government employment, including the interviewing of individuals for employment.

(10) The approval of position descriptions and performance standards for Federal employees.

(11) The determination of what Government property is to be disposed of and on what terms (although an agency may give contractors authority to dispose of property at prices within specified ranges and subject to other reasonable conditions deemed appropriate by the agency).

(12) In Federal procurement activities with respect to prime contracts—

(i) Determining what supplies or services are to be acquired by the Government (although an agency may give contractors authority to acquire supplies at prices within specified ranges and subject to other reasonable conditions deemed appropriate by the agency);

(ii) Participating as a voting member on any source selection boards;

(iii) Approving any contractual documents, to include documents defining requirements, incentive plans, and evaluation criteria;

(iv) Awarding contracts;

(v) Administering contracts (including ordering changes in contract performance or contract quantities, taking action based on evaluations of contractor performance, and accepting or rejecting contractor products or services);

(vi) Terminating contracts;

(vii) Determining whether contract costs are reasonable, allocable, and allowable; and

(viii) Participating as a voting member on performance evaluation boards.

(13) The approval of agency responses to Freedom of Information Act requests (other than routine responses that, because of statute, regulation, or agency

policy, do not require the exercise of judgment in determining whether documents are to be released or withheld), and the approval of agency responses to the administrative appeals of denials of Freedom of Information Act requests.

(14) The conduct of administrative hearings to determine the eligibility of any person for a security clearance, or involving actions that affect matters of personal reputation or eligibility to participate in Government programs.

(15) The approval of Federal licensing actions and inspections.

(16) The determination of budget policy, guidance, and strategy.

(17) The collection, control, and disbursement of fees, royalties, duties, fines, taxes, and other public funds, unless authorized by statute, such as 31 U.S.C. 952 (relating to private collection contractors) and 31 U.S.C. 3718 (relating to private attorney collection services), but not including—

(i) Collection of fees, fines, penalties, costs, or other charges from visitors to or patrons of mess halls, post or base exchange concessions, national parks, and similar entities or activities, or from other persons, where the amount to be collected is easily calculated or predetermined and the funds collected can be easily controlled using standard case management techniques; and

(ii) Routine voucher and invoice examination.

(18) The control of the treasury accounts.

(19) The administration of public trusts.

(20) The drafting of Congressional testimony, responses to Congressional correspondence, or agency responses to audit reports from the Inspector General, the Government Accountability Office, or other Federal audit entity.

(d) The following is a list of examples of functions generally not considered to be inherently governmental functions. However, certain services and actions that are not considered to be inherently governmental functions may approach being in that category because of the nature of the function, the manner in which the contractor performs the contract, or the manner in which the Government administers contractor performance. This list is not all inclusive:

(1) Services that involve or relate to budget preparation, including workload modeling, fact finding, efficiency studies, and should-cost analyses, etc.

(2) Services that involve or relate to reorganization and planning activities.

(3) Services that involve or relate to analyses, feasibility studies, and strategy options to be used by agency personnel in developing policy.

(4) Services that involve or relate to the development of regulations.

(5) Services that involve or relate to the evaluation of another contractor's performance.

(6) Services in support of acquisition planning.

(7) Contractors providing assistance in contract management (such as where the contractor might influence official evaluations of other contractors).

(8) Contractors providing technical evaluation of contract proposals.

(9) Contractors providing assistance in the development of statements of work.

(10) Contractors providing support in preparing responses to Freedom of Information Act requests.

(11) Contractors working in any situation that permits or might permit them to gain access to confidential business information and/or any other sensitive information (other than situations covered by the National Industrial Security Program described in 4.302(b)).

(12) Contractors providing information regarding agency policies or regulations, such as attending conferences on behalf of an agency, conducting community relations campaigns, or conducting agency training courses.

(13) Contractors participating in any situation where it might be assumed that they are agency employees or representatives.

(14) Contractors participating as technical advisors to a source selection board or participating as voting or nonvoting members of a source evaluation board.

(15) Contractors serving as arbitrators or providing alternative methods of dispute resolution.

(16) Contractors constructing buildings or structures intended to be secure from electronic eavesdropping or other penetration by foreign governments.

(17) Contractors providing inspection services.

(18) Contractors providing legal advice and interpretations of regulations and statutes to Government officials.

(19) Contractors providing special non-law enforcement, security activities that do not directly involve criminal investigations, such as prisoner detention or transport and non-military national security details.

Attachment B: Department of Defense UAS Platforms

Table I. DoD UAS Platforms				
Name	**Vehicles**	**Ground Control Stations**	**Employing Service(s)**	**Capability/Mission**
RQ-4A Global Hawk/BAMS-D Block 10	9	3	USAF/Navy	ISR/Maritime Domain Awareness (Navy)
RQ-4B Global Hawk Block 20/30	15	3	USAF	ISR
RQ-4B Global Hawk Block 40	1	1	USAF	ISR/Battle Management Command & Control
MQ-9 Reaper	54	61*	USAF	ISR/Reconnaissance, Surveillance, and Target Acquisition/EW/ Precision Strike/Force Protection
MQ-1 A/B Predator	161	61*	USAF	ISR/Reconnaissance, Surveillance, and Target Acquisition/Precision Strike/Force Protection (MQ-1C Only-C3/LG)
MQ-1 Warrior/ MQ-1C Gray Eagle	26	24	Army	ISR/Reconnaissance, Surveillance, and Target Acquisition/Precision Strike/Force Protection (MQ-1C Only-C3/LG)
UCAS-D	2	0	Navy	Demonstration Only
MQ-8B Fire Scout VTUAV	9	7	Navy	ISR/Reconnaissance, Surveillance, and Target Acquisition/Anti-Submarine Warfare/ASUW/MIW/ OMCM
MQ-5 Hunter	25	16	Army	ISR/Reconnaissance, Surveillance, and Target Acquisition/Battle Damage Assessment
RQ-7 Shadow	364	262	Army USMC/ SOCOM	ISR/Reconnaissance, Surveillance, and Target Acquisition/Battle Damage Assessment
A160T Hummingbird	8	3	SOCOM/DARPA/ Army	Demonstration
STUAS	0	0	Navy/USMC	ISR/Explosive Ordinance Disposal/ Force Protection
Scan Eagle	122	39	Navy/SOCOM	ISR/Reconnaissance, Surveillance, and Target Acquisition/Force Protection
RQ-11 Raven	5346	3291	Army/Navy/ SOCOM	ISR/Reconnaissance, Surveillance, and Target Acquisition
Wasp	916	323	USMC/ SOCOM	ISR/Reconnaissance, Surveillance, and Target Acquisition
SUAS AECV Puma	39	26	SOCOM	ISR/Reconnaissance, Surveillance, and Target Acquisition
gMAV / T-Hawk	377	194	Army (gMAV) Navy (T-Hawk)	ISR/Reconnaissance, Surveillance, and Target Acquisition/Explosive Ordinance Disposal

Source: Weatherington brief.
Note: For comparison purposes, table does not include mini/small, micro, or lighter-than-air UAS.
a. MQ-1 and MQ-9 use the same GCS.

INFORMATION FOR CONTRIBUTORS

The Air Force Law Review publishes articles, notes, comments, and book reviews. The Editorial Board encourages readers to submit manuscripts on any area of law or legal practice that may be of interest to judge advocates and military lawyers. Because the *Law Review* is a publication of The Judge Advocate General's Corps, USAF, Air Force judge advocates and civilian attorneys are particularly encouraged to contribute. Authors are invited to submit scholarly, timely, and well-written articles for consideration by the Editorial Board. The *Law Review* does not pay authors any compensation for items selected for publication.

Manuscript Review. Members of the Editorial Board review all manuscripts to determine suitability for publication in light of space and editorial limitations. Manuscripts selected for publication undergo an editorial and technical review, as well as a policy and security clearance as required. The Editor will make necessary revisions or deletions without prior permission of, or coordination with the author. Authors are responsible for the accuracy of all material submitted, including citations and other references. The *Law Review* generally does not publish material committed for publication in other journals. In lieu of reprints, authors are provided two copies of the issue containing their work.

Manuscript Form. Manuscripts may be submitted by disc or electronic mail in Microsoft Word format. Please contact the Editor at (334) 953-2802 for submission guidelines or contact the Editor at the address on the inside front cover and provide your electronic contact information. Authors should retain backup copies of all submissions. Footnotes must follow the format prescribed by A Uniform System of Citation (19th ed. 2010). Include appropriate biographical data concerning the author(s), such as rank, position, duty assignment, educational background, and bar affiliations. The Editorial Board will consider manuscripts of any length, but articles selected for publication are generally less than 60 pages of text. The *Law Review* does not return unpublished manuscripts.

Distribution. *The Air Force Law Review* is distributed to Air Force judge advocates. In addition, it reaches other military services, law schools, bar associations, international organizations, foreign governments, federal and state agencies, and civilian lawyers.


THE JUDGE ADVOCATE GENERAL'S SCHOOL
UNITED STATES AIR FORCE