IN THE UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES

UNITED STATES, Appellant	)	APPELLANT'S BRIEF IN SUPPORT OF CERTIFIED ISSUES, ERRATA CORRECTED
v.	)	
	)	Crim.App. Dkt. No. 202400253
Anderson A. IXCOLGONZALEZ, Corporal (E-4) U.S. Marine Corps, Appellee	)	USCA Dkt. No. 25-0243/MC

JACOB R. CARMIN
Captain, U.S. Marine Corps
Appellate Government Counsel
Navy-Marine Corps Appellate Review Activity
Bldg. 58, Suite B01
1254 Charles Morris Street SE
Washington Navy Yard, DC 20374
(202) 685-4623, fax (202) 685-7687
Bar no. 38092

MARY CLAIRE FINNEN
Major, U.S. Marine Corps
Senior Appellate Counsel
Navy-Marine Corps Appellate Review Activity
Bldg. 58, Suite B01
1254 Charles Morris Street SE
Washington Navy Yard, DC 20374
(202) 685-8502, fax (202) 685-7687
Bar no. 37314

IAIN D. PEDDEN
Colonel, U.S. Marine Corps
Director, Appellate Government
Navy-Marine Corps Appellate Review Activity
Bldg. 58, Suite B01
1254 Charles Morris Street SE
Washington Navy Yard, DC 20374
(202) 685-7427, fax (202) 685-7687
Bar no. 33211

BRIAN K. KELLER
Deputy Director
Appellate Government
Navy-Marine Corps Appellate Review Activity
Bldg. 58, Suite B01
1254 Charles Morris Street SE
Washington Navy Yard, DC 20374
(202) 685-7682, fax (202) 685-7687
Bar no. 31714

Index of Brief

Page

Table of Authorities

Page

UNITED STATES SUPREME COURT CASES

UNITED STATES COURT OF APPEALS FOR THE ARMED FORCES AND COURT OF MILITARY APPEALS CASES

UNITED STATES NAVY-MARINE CORPS COURT OF CRIMINAL APPEALS CASES

UNITED STATES CIRCUIT COURTS OF APPEALS CASES

Issues Presented

I.

DID THE MILITARY JUDGE ERR SUPPRESSING DIGITAL DEVICE EVIDENCE BECAUSE THE AUTHORIZATION DID NOT USE "AS MUCH SPECIFICITY AS THE GOVERNMENT'S KNOWLEDGE AND CIRCUMSTANCES" ALLOWED—WHEN *RICHARDS* REQUIRES ONLY ENOUGH TO PREVENT A SEARCH CLEARLY OUTSIDE THE SCOPE OF THE CRIME BEING INVESTIGATED, AND THE AUTHORIZATION SPECIFIED CHILD PORNOGRAPHY CRIMES AND EVIDENCE OF THOSE CRIMES?

II.

DID THE MILITARY JUDGE AND LOWER COURT ERR FINDING THAT GOOD FAITH DID NOT APPLY BECAUSE THE AUTHORIZATION DID NOT SPECIFY LOCATIONS TO BE SEARCHED INSIDE THE DIGITAL DEVICES, BASING THAT FINDING ON THE FOURTH AMENDMENT, WHERE "COMPUTER FILES MAY BE MANIPULATED TO HIDE THEIR TRUE CONTENT," AND WHERE THE RULE AT THE TIME OF THE SEARCH WAS THAT THE AUTHORIZATION WAS SUFFICIENT AND THE AFFIDAVIT WAS INCORPORATED?

III.

DID THE MILITARY JUDGE ERR HOLDING THAT THE AFFIDAVIT WAS NOT INCORPORATED WHERE THE AUTHORIZATION TWICE REFERENCED THE ATTACHED AFFIDAVIT SIGNED BY THE COMMANDING OFFICER AND WHERE MIL. R. EVID. 315 ONLY REQUIRES STATEMENTS IN SUPPORT OF PROBABLE CAUSE TO BE "COMMUNICATED," BUT DOES NOT REQUIRE WORDS OF INCORPORATION?

IV.

DID THE MILITARY JUDGE ABUSE HIS DISCRETION WHEN HE FOUND THAT LAW ENFORCEMENT WAS SUFFICIENTLY CULPABLE SUCH THAT THE EXCLUSIONARY RULE WOULD MEANINGFULLY DETER IT?

Statement of Statutory Jurisdiction

Pursuant to Article 62(a)(1)(B), Uniform Code of Military Justice (UCMJ), 10 U.S.C. § 862(a)(1)(B) (2024), the United States timely appealed the Military Judge's Ruling suppressing evidence resulting from a Command Authorization for Search and Seizure. This evidence is substantial proof of a fact material in the proceeding. On August 25, 2025, the Judge Advocate General of the United States Navy certified four Issues for review. This Court has jurisdiction under Article 67(a)(2), UCMJ, § 867(a)(2) (2024) .

Statement of the Case

The Convening Authority referred Charges against Appellee to a general court-martial, alleging possession of child pornography, distributing child pornography, receiving child pornography, and soliciting distribution of child pornography, in violation of Articles 82 and 134, UCMJ, 10 U.S.C. §§ 882, 934. The Military Judge issued a Ruling suppressing evidence resulting from a Command Authorization for Search and Seizure. The United States timely appealed the Ruling.

On review, the lower court heard oral argument and issued an Opinion on April 30, 2025, affirming the Military Judge's Ruling. *United States v. Ixcolgonzalez*, No. 202400253, 2025 CCA LEXIS 186 (N-M. Ct. Crim. App. Apr. 30, 2025). The United States moved for panel and *en banc* reconsideration on May 30, 2025. (J.A. 105). The lower court denied the Motion on June 24, 2025. (Order Den. Recons., Jun. 24, 2025).

Summary of Argument

The Military Judge and lower court erred by adopting a standard that search authorizations must use "as much specificity as the government's knowledge and circumstances allow" citing language—but not the holding—in *United States v. Richards*, 76 M.J. 365, 369 (C.A.A.F. 2017). The Authorization here affirmatively limited the search to evidence of specific federal crimes and was thus valid.

Regardless, law enforcement acted in good faith reliance on the Authorization, as the commander reviewed the sworn Affidavit and Authorization contemporaneously, and law enforcement had no reason to believe the Authorization did not establish a substantial basis for probable cause.

The Authorization was sufficiently particular, but even if it was not, it incorporated the Affidavit, which had greater particularity. The Military Judge should have construed the Authorization in light of the detailed affidavit because the Authorization contained words of incorporation and the commander signed both documents.

Finally, the Military Judge also erred by finding a speculative deterrent effect, hypothetically motivating law enforcement and authorizing officials from failing to adhere to the particularity requirement, outweighed the substantial costs of excluding more than five-hundred digital files containing potential child pornography.

Statement of Facts

A. The United States charged Appellee with possession, distribution, soliciting distribution, and receiving child pornography.

The United States charged Appellee with one Specification of possession of child pornography, six Specifications of distributing child pornography, one Specification of receiving child pornography, and one Specification of soliciting

distribution of child pornography in violation of Articles 82 and 134, UCMJ. (J.A. 136–139.)

B. Appellee moved to suppress evidence resulting from a Command Authorization for Search and Seizure.

1. In a Motion to Suppress, Appellee argued the Authorization was overly broad, the Affidavit was not incorporated in the Authorization, and that suppression would deter commanders from signing vague authorizations and prevent law enforcement from straying outside authorized limits.

Appellee moved to suppress all evidence derived from his digital devices because the Command Authorized Search and Seizure "was overly broad and failed to specify targeted devices, leading to an overly broad scope of the search." (J.A. 217.) He argued the term "digital devices" was too broad and that law enforcement did not have "substantial basis for seizing any of the digital devices." (J.A. 220.) "By keeping the [CASS] in such a vague state," Appellee argued, law enforcement was empowered "to access far beyond what that prescribed in the Fourth Amendment." (J.A. 222.)

Appellee further claimed the Authorization was facially invalid because the Affidavit was not incorporated. (J.A. 198, 220.) He argued suppression would result in appreciable deterrence because it would "deter commanders from granting vague and rushed authorizations . . . and dissuade law enforcement from straying outside the limits of any granted authorizations." (J.A. 190.) He argued the deterrent impact would be "significant" because "[t]hese are parties who have can

be expected to have regular contact with the military justice system, investigations, and the search of electronic devices." (J.A. 227.)

2. The CASS and Affidavit showed that the investigation started as a Snapchat-generated Cybertip to NCMEC.

As Enclosures to his Motion, Appellee included the Authorization and Affidavit. Agent Lawrence, Naval Criminal Investigative Service, applied for a Command Authorization for Search and Seizure with an Affidavit in Support of Application. (J.A. 268).

Agent Lawrence described the probable cause in the Affidavit. Law enforcement received and reviewed a National Center for Missing and Exploited Children (NCMEC) CyberTipline Report from the Internet Crimes Against Children Data System. (J.A. 268.) Snapchat generated the tip and reported user "agoku70." (J.A. 268.) Snapchat also submitted a file and the user's phone number and Internet Protocol address. (J.A. 268.) The file contained a video of "an unknown person, using his/her hand to masturbate the penis of a prepubescent male, whom [sic] appeared to be approximately [ten-] to [thirteen-]years-old." (J.A. 275.) In response to a search warrant, Snapchat provided four more videos of apparent minors engaged in sexual activity. (J.A. 275.)

Agent Lawrence then requested authorization to "seize and search" "[a]ny and all computer, mobile or storage media devices capable of storing digital files" located in Appellee's barracks room and on his person, pertaining to his suspected

possession and distribution of child pornography. (J.A. 268, 278.) Agent Lawrence also requested to "search" Appellee's "seized" "devices" for "Snapchat . . . ; Presence of [Appellee's] email address . . . ; Child pornography . . . ; Proof of ownership . . . ; [*a*]*ny and all applications* of which videos and photographs are stored *or records thereof*." (J.A. 278 (emphasis added).) Agent Lawrence requested permission to "search" Appellee's "cellular device, in any application or folders where photographs and videos may be stored." (J.A. 278.)

3. Appellee's Commanding Officer signed the Affidavit and the Command Authorization for Search and Seizure.

On August 17, 2022, Appellee's Commanding Officer signed both the Affidavit in Support and the Command Authorization for Search and Seizure. (J.A. 279–280.) Recognizing "Affidavit(s) having been made before [him] by Special Agent [Lawrence]," the Commanding Officer "AUTHORIZED [law enforcement] TO SEARCH" for "[e]vidence of violations of Article 134 (Possession, receiving, or viewing of child pornography) and Article 134 (Distribution of Childing Pornography) of the Uniform Code of Military Justice," which could be found in "[d]igital devices belonging to [Appellee] and [Appellee's] . . . [b]arracks . . . [r]oom," and "if the property is found there to seize it. . . ." (J.A. 280.)

4. Law enforcement seized Appellee's digital devices.

Special Agent Lawrence testified about the CASS. (J.A. 154.) He served the Command Authorization for Search and Seizure on Appellee. (J.A. 151.) Appellee's Apple iPhone was seized from where it had been stored at the NCIS building prior to his entry into the interrogation room. (J.A. 170.) Law enforcement then searched Appellee's barracks room and seized additional digital devices, including his laptop, Motorola cell phone, computer tower, and a hard drive. (J.A. 151, 237, 282.)

The Agent explained that while "electronic devices" might technically include a microwave or a coffeemaker, he wouldn't have seized such a device because he was only searching for digital devices that were likely to have contraband. (J.A. 154.) Specifically, he was searching for "computers, cell phones, any kind of digital media . . . that stores contraband, hard drives . . . ." (J.A. 157.) For example, he wouldn't have seized an alarm clock because "you can't store the kind of content we were looking for on an alarm clock." (J.A. 157.)

5. The Digital Analyst searched the digital devices and found evidence of child pornography.

Naval Criminal Investigative Service sent the digital devices to the Department of Defense Cyber Crimes Center Cyber Forensic Laboratory ("DC3"). (J.A. 205, 237.) Agent Lawrence asked the Digital Analyst to "recover and analy[ze] the following items:"

- Identify items pertaining to the suspected violations of Article 134 [Possessing, receiving, or viewing Child Sexual Abuse Material (CSAM)] and Article 134 (Distribution of Child Pornography) of the Uniform Code of Military Justice (UCMJ).

- Snapchat messaging application pertaining to the above mentioned violations of the UCMJ.

- Presence of the email address [email address omitted].

- Proof of ownership of the submitted evidence items.

- Any and all applications in which videos and/or photographs are stored or records of.

(J.A. 206.)

The Digital Analyst found 254 video files and 272 picture files in Appellee's iPhone that were "potential CSAM," including one video file associated with the NCMEC database, four files matching the NCMEC tip, and sixty-three messages "requesting, sending, and/or receiving potential CSAM." (J.A. 206.)

C. The United States argued that the Authorization limited the nature of evidence to be seized and incorporated the Affidavit, that suppression had no deterrence value, and that the good faith exception applied.

The United States responded that the Authorization did not lack particularity; the term "digital devices" within the CASS was "sufficiently specific" because it was limited by the nature of the evidence to be seized. (J.A. 263.) The United States also argued that under *United States v. Richards,* 76 M.J. 365 (C.A.A.F. 2017), the Authorization was permissibly "expansive enough to allow investigators access to the places where incriminating materials may be

hidden." (J.A. 261.) Further, the Affidavit was incorporated into the Authorization and paragraphs twenty-nine though thirty-five of the Affidavit provided "more details about why and where the NCIS [sic] expects to find evidence of these crimes." (J.A. 196–197.)

D. The Military Judge suppressed the evidence.

The Military Judge granted Appellee's Motion and suppressed the evidence. (J.A. 393.)

1. The Military Judge made Findings of Fact.

The Military Judge made Findings of Fact. (J.A. 393.) He found that Agent Lawrence "briefed" the Commanding Officer, provided him with a copy of the CASS and the Affidavit, and swore an oral declaration of probable cause. (J.A. 394.) The Military Judge thus "infer[red]" that the CASS had been prepared for the Commanding Officer by Agent Lawrence. (J.A. 394.) The Military Judge found that the Affidavit should be interpreted as a request to "seize the accused's digital devices," and search two "places" within the device: "Snapchat social media messaging application pertaining to the mentioned violations of the UCMJ," and "Any and all applications in which videos and photographs are stored or records thereof," (J.A. 394.) Within those places, the Military Judge believed that the search was limited to "child pornography images and videos," "proof of

ownership of the mobile/computer devices seized," and "presence of the email address [address omitted]." (J.A. 394.)

The Military Judge then found that the signed Authorization did not include the items listed in the Affidavit, either expressly or by reference. (J.A. 394.) However, he found that Agent Lawrence's search request to DC3 was nearly identical to the specified list from the Affidavit. (J.A. 396.)

With respect to the digital forensic search, the Military Judge found that six video files were "cache files," automatically created by the operating system after viewing, three image files were located in the "Digital Camera Images folder (DCIM)," the default location for videos and images to be saved on mobile phones. (J.A. 396.) The remaining images and videos had file paths consistent with the Telegram app's media storage. (J.A. 396.)

2. The Military Judge held the Authorization lacked sufficient particularity because the Government could have provided more particularity based on the Affidavit.

The Military Judge held the Command Authorization "lack[s] sufficient particularity with regard to the places—that is, the data—to be searched within the accused's digital devices," and the things to be seized—"whether that be digital pictures depicting child pornography, digital video files depicting child pornography, communications between the accused and another establishing the receipt or distribution of child pornography, something else, or all of these things."

(J.A. 398–99.) The Military Judge found that "the search authorization marginally satisfies the particularity requirement with respect to the things being seized. The search authorization articulates that the following evidence is being concealed: Evidence of violations of Article 134 (Possession, receiving, or viewing of child pornography) and Article 134 (Distribution of Child Pornography) of the Uniform Code of Military Justice." (J.A. 398 n.38.)

First, the Military Judge held:

> (1) it was reasonable for the commander to provide a *more* specific description of the types of data within the accused digital devices that law enforcement were permitted to search; (2) the search authorization fell well-short of as much specificity as the government's knowledge and circumstances allowed; and (3) limiting the warrant to the specificity particularly known by the government would *not* have unduly restricted the government's search objectives.

(J.A. 400 (emphasis in original).)

Second, the Military Judge held that the "most obvious deficiency" with the authorization was the "lack of particularity with respect to the places—that is, the data—to be searched within the digital devices." (J.A. 398.) He found the CASS lacked any particularity as to "the types of data, the data sets, or the applications withing the devices that can be searched." (J.A. 398–399.)

The Military Judge held that "had the [Command Authorization] been limited in scope to the particularity known by the government and as conveyed through the supporting [A]ffidavit, such particularity would not have restricted the

government's search objectives" because the Digital Analyst "undoubtedly relied upon the specificity of [Agent Lawrence's] request which was nearly identical to the items to be search and seized within [the Affidavit]." (J.A. 400.)

Nonetheless, the Military Judge found that the Command Authorization was sufficiently particular with regard to seizure of the "digital devices. . . . It was not reasonable for the [C]ommander to provide a specified list of the digital devices to be seized and searched because at the time law enforcement sought the [Command Authorization], the [G]overnment was unaware of the type and quantity of the digital devices possessed by [Appellee]—but the [G]overnment certainly had probable cause to believe that [Appelee] used a digital device to commit the alleged crimes." (J.A. 398 n.39.)

Lastly, the Military Judge found the good faith exception did not apply. (J.A. 406.) Reasoning that "because the particularity requirement exists in the text of the U.S. Constitution, and is not the product of some hyper-technical legal interpretation of Fourth Amendment jurisprudence," he held no reasonable officer could find the CASS valid. (J.A. 407.) The Military Judge found suppression would result in appreciable deterrence to "law enforcement agents . . .who prepare requests for search authorizations, and commanders who authorize searches, from failing to adhere to the particularity requirement prescribed by the text of the Fourth Amendment." (J.A. 408.) The Military Judge stated that the Commanding

Officer had failed to "strike an appropriate balance" between "being expansive enough to allow investigators access to places where incriminating evidence may be hidden, yet not so broad that they become the sort of free-for-all general searches the Fourth Amendment was designed to prevent." (J.A. 408.)

E. The lower court found that the Military Judge did not abuse his discretion because "digital devices" was overbroad, and the Commanding Officer did not use "as much specificity as the government's knowledge and circumstances allowed."

The lower court found the authorization was not facially valid, concluding that this Court had adopted a standard that required authorizations to include "as much specificity as the government's knowledge and circumstances allow." (J.A. 5.) While the Military Judge required particularity to limit the search within the digital devices, the lower court instead primarily focused on the term "digital devices" as overbroad. (J.A. 5.) The lower court found the term included items like refrigerators and washing machines and resulted in fatal overbreadth. (J.A. 6.)

The service court also found the Affidavit was not incorporated by reference because the form language was not unequivocal. (J.A. 6–10.) The lower court distinguished *Baranski v. Fifteen Unknown Agents of the BATF*, 452 F. 3d 433, 443 (6th Cir. 2006), from the present case because the *Baranski* warrant used the words "See Attached Affidavit." The Court of Criminal Appeals found the two references to the Affidavit here—stating "Affidavit(s) having been made before me" and "as stated in the supporting affidavit(s)"—were mere "boilerplate" and

thus did not operate in the same manner as did the references in *Baranski*. (J.A. 8–9)

The lower court held that the good faith exception did not apply because the Authorization was so facially deficient that an agent could not reasonably presume it to be valid. (J.A. 14.) Additionally, it rejected the United States' argument that the exclusionary rule did not apply, reasoning that the exclusion was sufficient to deter the "habitual" use of twenty-five-year-old boilerplate language in the CASS form. (J.A. 14.) The Court affirmed the Military Judge's ruling and denied the United States' appeal. (J.A. 15.)

In a dissenting Opinion, Judge Gannon opined that the Military Judge "misapprehended the distinction between a search authorization and a search warrant" under Mil. R. Evid. 315. (J.A. 16.) He noted that Mil. R. Evid. 315 "does not contain any requirement that the search authorization must contain 'appropriate words of incorporation' in order for the authorizing official to consider… statements in assessing probable cause[,]" that the "President has occupied the field with respect to what may be considered in support of a search authorization[,]" and that "[u]ntil our Superior Court specifically requires 'appropriate words of incorporation' in the context of search authorizations, Rule 315 controls." *Id.* at *29–31.

Argument

I.

RICHARDS REQUIRES ONLY THAT AN AUTHORIZATION BE PARTICULAR ENOUGH TO PREVENT A SEARCH CLEARLY OUTSIDE THE SCOPE OF THE CRIME BEING INVESTIGATED. THE AUTHORIZATION LIMITED THE SEARCH TO PLACES ON DIGITAL DEVICES WHERE EVIDENCE OF CHILD PORNOGRAPHY CRIMES WERE LIKELY TO BE FOUND. THE MILITARY JUDGE AND LOWER COURT ERRED BY RELYING ON SINCE-ABANDONED TENTH CIRCUIT PRECEDENT REQUIRING EX ANTE SPECIFICITY FOR DIGITAL DEVICE SEARCHES.

A. Standard of review.

Courts review a military judge's ruling on a motion to suppress evidence for an abuse of discretion. *United States v. Harborth*, 24-0124, 24-0125, 2025 CAAF LEXIS 436 at *14 (C.A.A.F. June 3, 2025). This Court "typically pierc[es] through [the] intermediate level and examin[es] the military judge's ruling, then decide[s] whether the Court of Criminal Appeals was right or wrong in its examination of the military judge's ruling." *Id.* In an Article 62 appeal, courts review evidence in the light most favorable to the party that prevailed at trial. *Id.*

An abuse of discretion occurs when the trial court's findings of fact are clearly erroneous or if the court's decision is influenced by an erroneous view of the law. *Id*. On questions of fact, the court is "limited to determining whether the

military judge's findings are clearly erroneous or unsupported by the record." *United States v. Lincoln*, 42 M.J. 315, 320 (C.A.A.F. 1995).

B. The Military Judge abused his discretion. Contrary to *Richards*, he incorrectly conflated the standards for the particularity of an authorization and the reasonableness of a search's execution—leading him to find the Command Authorization was not "sufficiently particular." Consistent with *Shields*, the Digital Analyst reasonably searched the digital devices.

1. The Warrant Clause of the Fourth Amendment requires that a warrant be sufficiently particular.

"The Warrant Clause of the Fourth Amendment categorically prohibits the issuance of any warrant except one 'particularly describing the place to be searched and the persons or things to be seized.'" *Maryland v. Garrison*, 480 U.S. 79, 84 (1978) (citing U.S. Const. amend. IV).

The purpose of this particularity requirement was "to prevent general searches." *Id*. "By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searchers the Framers intended to prohibit." *Id*.

The Court of Appeals for the Armed Forces echoed this: "[t]he Fourth Amendment requires that a search warrant describe the things to be seized with *sufficient particularity* to prevent a general exploratory rummaging in a person's

belongings." *United States v. Richards*, 76 M.J. 365, 369 (C.A.A.F. 2017) (emphasis added).

2. *Richards* and most federal circuits reject narrow ex ante limitations on digital searches because computer files, unlike physical files, can be manipulated to hide their true contents, and because there may be no substitute for looking in all folders for the evidence.

    a. Although the court in *Richards* considered a circuit case requiring "affirmatively limit[ing]" searches of digital devices, it instead upheld an authorization because it "did not give authorities carte blanche to search in the areas clearly outside the scope of the crime being investigated."

"A search warrant does not necessarily lack particularity simply because it is broad." *United States v. Purcell*, 967 F.3d 159, 179 (2d Cir. 2020) (internal citations omitted). The *Richards* court summarized that in the context of electronic devices, courts must not be overly restrictive and instead achieve a balance. 76 M.J. at 369. Although "'warrants for computer searches must affirmatively limit the search to evidence of specific federal crimes or specific types of material,' we also recognize the dangers of too narrowly limiting where investigators can go." *Id*. at 370 (quoting *United States v. Riccardi*, 405 F.3d 852, 862 (10th Cir. 2005)). The court also considered that where computer image files were concerned, "[t]here may be no practical substitute for actually looking in many (perhaps all) folders and sometimes at the documents contained within those folders . . ." *Id*.

(internal quotation marks omitted) (quoting *United States v. Burgess*, 576 F.3d 1078, 1094 (10th Cir. 2009)).

The *Richards* Court thus rejected imposing narrow *ex ante* restrictions on how searches are conducted inside digital devices. 76 M.J. at 370. It departed from the Tenth Circuit approach in *Riccardi* and explained: "Unlike a physical object that can be immediately identified as responsive to the warrant or not, computer files may be manipulated to hide their true contents." *Richards*, 76 M.J. at 370 (internal quotation marks omitted) (quoting *United States v. Mann*, 592 F.3d 779, 782 (7th Cir. 2010)). It upheld an authorization that did not have a temporal limitation even when that information was known to investigators because "the authorization was already sufficiently particularized to prevent a general search." 76 M.J. at 370. The court found sufficient particularity where the authorization did not give law enforcement "carte blanche to search in areas clearly outside the scope of the crime being investigated." *Id.*

b. The Military Judge and the lower court misapprehended *Richards*: the Fourth Amendment test is not that authorizations are insufficient where it "would have been reasonable to provide a more specific description of locations inside digital devices."

The Military Judge held "it was reasonable for the commander to provide a *more* specific description of the types of data within the accused's digital devices," and that "limiting the warrant to the specificity particularity known by the

government would *not* have unduly restricted the government's search objectives. (J.A. 400 (emphasis in original).) Further, the Military Judge held that the Command Authorization should have been as specific as the Affidavit. (J.A 400.)

The lower court affirmed the ruling, reasoning that this Court "has seemingly adopted the Tenth Circuit Court of Appeals' rationale that warrants must use "as much specificity as the government's knowledge and circumstances allow." (J.A. 5.)

The Military Judge and the lower court erred because that is not the test. *See supra*, Section I.B.2.a. This Court has not established the test that a warrant is not particularized if it would have been "'reasonable to provide a more specific description' of the location" on the digital device itself. Thus, the Military Judge's statement, adopted by the lower court, that the authorization was invalid because it was reasonable to have incorporated additional detail is also an incorrect application of the law. (J.A. 6–7, 400.)

The United States is unaware of any precedent that would support such a heightened reasonableness standard for the particularity requirement or requiring that command authorizations contain recitations of supporting affidavits. Instead, the *Richards* court held it was sufficient that the command authorization restricted the search to the "[a]ppellant's electronic media for any communication that related to his possible violation of the Florida statute in his relationship with [the

victim]." *Id*. The standard applied to electronic devices must "allow investigators access to places where incriminating materials may be hidden, yet not so broad that they become the sort of free-for-all general searches the Fourth Amendment was designed to prevent." *Id*.

The Military Judge's belief that the Command Authorization "gave law enforcement the authority to search everything on the defendant's electronic devices in the hopes of finding anything, but nothing in particular, that could help in the investigation," thus contradicts the standard and analysis established by the Court in *Richards*. (J.A. 402); *see Richards*, 76 M.J. at 370. Further, the lower court was incorrect in concluding that this Court in *Richards* adopted the standard in *Riccardi*.

Like *Richards*, the Command Authorization alone is "sufficiently particular[]" to prevent a general exploratory rummaging in a person's belongings. 78 M.J. at 368, 371; *see Garrison*, 480 U.S. at 84.

c. The lower court's erroneous interpretation of the Fourth Amendment is inconsistent with other federal precedent that rejects the imposition of narrow, ex ante limitations as to how searches inside digital devices should be conducted.

The majority of federal circuits, like the Court in *Richards*, disfavor restrictions on digital searches like temporal limitations and ex ante imposing search methodologies—like where to look on devices or how to conduct

searches—on electronic devices; instead, warrants and authorizations need only be "sufficiently particularized to prevent a general search." 76 M.J. at 367, 370. Indeed, federal appellate courts take a broad approach to searches of electronic devices, files, and folders pursuant to a warrant, declining to apply the sort of restrictions to such searches the Military Judge and lower court did here.[1]

While this Court in *Richards* supported the concerns of the Tenth Circuit that warrants should "limit a search to . . . specific federal crimes or specific types of material," the Court rejected imposing *ex ante* restriction s because it "recognized the dangers of too narrowly limiting where investigators can go." 76 M.J. at 370. Other courts likewise find the degree of particularity constitutional when the description defines a search with "practical accuracy rather than absolute precision." *See United States v. Tompkins*, 118 F.4th 280, 287–88 (2d Cir. 2024) (collecting cases).

---

[1] *See United States v. Adjani*, 452 F.3d 1140, 1150 (9th Cir. 2006) (finding that because computer files are easily disguised, if the court restricted the warrant solely to specific search protocols [e.g., key word searches], much evidence could escape discovery simply because of the defendants' labeling of the files. *Burgess*, 576 F.3d at 1092–94 ("[T]here may be no practical substitute for actually looking in many (perhaps all) folders[.]"); *Mann*, 592 F.3d at 782 (relevant files are often hidden and can be mislabeled and "manipulated to hide their true contents"); *Williams*, 592 F.3d at 522 (where a warrant authorized a computer search for evidence of harassment, the agent was authorized to review *every file on the computer*); *United States v. Grubbs*, 547 U.S. 90, 99 (2006); *United States v. Hill*, 459 F.3d 966, 977 (9th Cir. 2006); *Guest v. Leis*, 255 F.3d 325, 334–35 (6th Cir. 2001); *United States v. Brooks*, 427 F.3d 1246, 1251 (10th Cir. 2005); *United States v. Upham*, 168 F.3d 532, 537 (1st Cir. 1999).

In *United States v. Smith*, 108 F. 4th 872 (D.C. Cir. 2024), the court considered the appellant's claims that the warrant was not sufficiently particular where it authorized search and seizure of "cellular phones, computers, digital storage devices, thumb drives, removable electronic devices . . . and any items or materials relating to the offense of First-Degree Child Sexual Abuse." *Id*. at 876. Because the suspected conduct included exchange of sexually abusive text messages and photos with a minor, the conduct "undoubtedly involved multiple electronic devices: namely, the cell phones [the minor and suspect] used to communicate with each other." *Id*. at 879. The *Smith* court declined to "hold that police officers armed with information that Smith stored evidence of his crimes on phones and personal computers were obligated to strictly conform the parameters of their investigation to the precise information recalled and related by [the minor victim]." *Id*.

Likewise, in *United States v. Corleto*, 56 F.4th 169 (1st Cir. 2022), the warrant authorized the search of appellant's home and cars for "records and visual depictions of minors engaged in sexually explicit conduct" and authorized the seizure of "any computer that was or may have been used to commit the offenses described on the warrant." *Id*. at 173. The definition of a computer in the warrant included smartphones, and an attachment listed items to be seized as "any computer or electronic media that were or may have been used as a means to

commit the offenses described on the warrant, including the production, receipt, possession, distribution, or transportation of child pornography." *Id*. The court understood the appellant to be arguing that "warrants targeting smartphones categorically require some greater standard of particularity than might otherwise be required." *Id.* at 176. Without deciding whether a higher standard should be applied, the *Corleto* court found the warrant sufficiently particular to "satisfy whatever heightened standard might reasonably apply to warrants targeting cell phones." *Id*.

Thus, both the Military Judge and the lower court erred in applying a higher standard of particularity for cell phone searches without support from this Court or federal circuit precedent.

d. The lower court and Military Judge erred in relying on the Tenth Circuit precedent cited in *Richards*—because even under that precedent, the Authorization here was sufficiently particular and that precedent has since been undermined by other Tenth Circuit cases.

While this Court in Richards agreed with the Tenth Circuit that general warrants are forbidden, it departed from the Tenth Circuit approach in *Riccardi*. *Riccardi,* in turn, developed from *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999).

In *Carey*, the court found no particularity issue with the warrant that broadly authorized the search of files on the computers for "names, telephone numbers,

ledger receipts, addresses, and other documentary evidence pertaining to the sale and distribution of controlled substances." 172 F.3d at 1270. Thus, the case that *Riccardi* relies on rejects a particularized description of the "location" *inside* the digital device and instead focused on the "items" sought.

In *Carey*, the court declined to apply the plain view exception when law enforcement searched image files for child pornography, which deliberately exceeded the scope of a warrant authorizing a search for evidence of drug trafficking only. 172 F.3d at 1270. Nonetheless, that court found no particularity issue with the warrant that broadly authorized the search of files on the computers for "names, telephone numbers, ledger receipts, addresses, and other documentary evidence pertaining to the sale and distribution of controlled substances." *Id.* Thus, the case that *Riccardi* relies on rejects a particularized description of the "location" *inside* the digital device and instead focused on the "items" sought. *Id*.

Moreover, the Tenth Circuit has since distanced itself from the *Riccardi* approach to ex ante digital search restrictions. *See United States v. Brooks*, 427 F.3d 1246, 1251 (10th Cir. 2005) (search warrants should not "contain a particularized computer search strategy" as to how devices will be searched for evidence of specified crimes); *see also United States v. Williams*, 592 F.3d 511, 519 (4th Cir. 2010) (rejecting position in *Carey* that suggests that during warranted search, any discovery of unauthorized evidence be inadvertent); *United States v.*

Stabile, 633 F.3d 219, 238–39 (3rd Cir. 2011). Thus, the Military Judge and lower court erred when they applied an ex ante restriction to the authorization.

e. The lower court also misapplied the Sixth Circuit precedent in this court's *Richards* opinion.

The Sixth Circuit in *United States v. Richards*, 659 F.3d 527 (6th Cir. 2011), also rejects *Riccardi*'s—and thus the Military Judge's and lower court's—approach. There, the court held that the warrant listing the server to be searched and the items to be seized presented no ambiguity—the warrant properly authorized the search and seizure of the entire server. 659 F.3d at 540. Here, the lower court replaced the Sixth Circuit's statement that the "proper metric" required specificity as to "items" with a rephrasing that claimed both *Richards* cases required specificity as to "location" on digital devices. (J.A. 6.). Simply put, *Richards,* and the majority of circuits, *reject* the lower court's claim that particularity is required under the Fourth Amendment as to *where* searchers may search *inside* digital devices.

3. The execution of a search authorization is reviewed for reasonableness.

"[T]he manner in which a warrant is executed is subject to later judicial review as to its reasonableness." *Dalia v. United States*, 441 U.S. 238, 258 (1979); *Shields*, 83 M.J. 226 (C.A.A.F. 2023). Searches conducted after obtaining a

warrant or authorization based on probable cause are presumptively reasonable. *United States v. Gurczynski*, 76 M.J. 381, 386 (C.A.A.F. 2017).

"Instead of attempting to set out bright line rules of limiting searches of electronic devices, the courts have looked to what is reasonable under the circumstances." *Shields*, 83 M.J. at 231. When it comes to searches of cellular phones and computers, "a search method is not unreasonable simply because it is not optimal." *Id*. at 232.

4. In the execution of the digital search, the Digital Analyst reasonably stayed within the scope of the authorization under *Shields*.

In *Shields*, law enforcement initially investigated the appellant for indecent exposure to Marine recruits. *Id*. at 228. To confirm the appellant's whereabouts, law enforcement obtained a search authorization permitting a search for "all location data stored on [the appellant's] phone or within any application within the phone for 23 Dec [20]18." *Id.* Law enforced seized the phone and sent it to the Defense Cyber Crime Center for extraction. *Id*.

After failing to find relevant location data for the specified date in the "device locations" file category, the analyst broadened his search. *Id*. at 229. He then searched through the "images category," because based on his training and experience, he knew image files often contained global positioning system location information. *Id*. There, he discovered evidence of child pornography. *Id.*

The court gave weight to the analyst's expertise in conducting such searches and held that the digital analyst's methodology that led to the discovery of child pornography was reasonable. *Id*. at 234.

Like *Shields*, the Digital Analyst reasonably examined Appellee's digital devices in relying on his own expertise in executing such a search. *See* 83 M.J. at 234. The Military Judge's application of a strict requirement to narrowly stay within the scope of the Command Authorization is contrary to *Shields*. (J.A. 206, 400.)

II.

THE MILITARY JUDGE ERRED IN NOT APPLYING THE GOOD FAITH EXCEPTION; LAW ENFORCEMENT REASONABLY BELIEVED THAT THE SEARCH AUTHORIZATION WAS VALID, BASED ON PROBABLE CAUSE, AND LIMITED THE SEARCH TO EVIDENCE OF DISTRIBUTION AND POSSESSION OF CHILD PORNOGRAPHY.

A. Standard of review.

Appellate courts review a military judge's denial of a motion to suppress evidence for an abuse of discretion. *See United States v. White*, 67 M.J. 322, 328 (C.A.A.F. 2020).

B. Law enforcement executed the Command Authorization in good faith.

1. Mil. R. Evid 311 provides a three-prong test for the good faith exception in courts-martial.

The good faith exception provides that evidence obtained as a result of an unlawful search or seizure is admissible if: (1) the search resulted from an authorization issued by a competent official under Mil. R. Evid. 315(d); (2) the individual authorizing the search had a "substantial basis" for determining the existence of probable cause; and (3) the officials seeking and executing the authorization "reasonably and with good faith" relied on the issuance of the search authorization. Mil. R. Evid. 311(b)(3)(A)–(C) (2019). This rule was intended to incorporate the Supreme Court's good-faith decisions, and "should [be] construe[d] . . . in a manner consistent with those decisions, if possible." *United States v. Carter*, 54 M.J. 414, 420–21 (C.A.A.F. 2001). And, the rule "covers searches conducted in objectively reasonable reliance on appellate precedent existing at the time of the search." *United States v. Zodhiates*, 901 F. 3d 137, 143 (2nd Cir. 2018).

As to the first prong, Mil. R. Evid. 315(d) authorizes a commander to issue a search authorization so long as he is "impartial." Mil. R. Evid. 315(d)(1). The commander must perform his function in a neutral and detached manner, and cannot "merely serve as a rubber stamp for the police." *See Carter*, 54 M.J. at 419; *see also United States v. Leedy*, 65 M.J. 208, 217–18 (C.A.A.F. 2007).

The second prong, requiring a "substantial basis for determining probable cause," is different here than when reviewing the propriety of the magistrate's

issuance of a search authorization. *Carter*, 54 M.J. at 422. This Court examines the search authorization "through the eyes of a reasonable law enforcement official executing the search authorization." *Id*. The requirement for a substantial basis "is satisfied if the law enforcement official had an objectively reasonable belief that the magistrate had a 'substantial basis' for determining the existence of probable cause." *Id*. In other words, "the affidavit must not be intentionally or recklessly false, and it must be more than a 'bare bones' recital of conclusions." *Id*. A "bare bones" affidavit is "one in which, inter alia, sources of information are not identified, and conflicts and gaps in evidence are not acknowledged." *Leedy*, 65 M.J. at 212 (citing *Carter*, 54 M.J. at 422).

Finally, the third prong requires the officials seeking and executing the authorization to "reasonably and with good faith" rely on the search authorization. Mil. R. Evid. 311(b)(3)(C); *Carter*, 54 M.J. 420–22. This is an objective standard. *Id*. Officials lack objective good faith where they "know that the magistrate merely 'rubber stamped' their request, or when the warrant is facially defective." *Carter*, 54 M.J. at 421.

2. The Commanding Officer acted impartially and did not merely "rubber stamp" the search authorization. Appellee did not argue otherwise in the lower court, thus waiving that claim.

In *Leedy*, the Court of Appeals for the Armed Forces upheld a magistrate's probable cause determination, and found that the magistrate had acted in a neutral

and detached manner. *Leedy*, 65 M.J. at 217–18. The *Leedy* court noted that "there [was] no evidence that the magistrate had any generalized proclivity towards simply conceding search requests to investigators," had "evidently closely read the affidavit," and spoke with a legal advisor and another commanding officer before authorizing the search. *Id.*

Similarly here, there is no evidence that the Commanding Officer had a "generalized proclivity towards simply conceding search requests to investigators." Agent Lawrence presented the Commanding Officer with a lengthy Affidavit, to which he swore; after consideration, the Commanding Officer independently determined there was probable cause to authorize the search and signed both the Affidavit and Search Authorization. (J.A. 279–280.) Appellee did not make this argument with particularity either at trial or on appeal, and has thus waived any claim to the contrary. *See United States v. Perkins*, 78 M.J. 381, 390 (C.A.A.F. 2019) (failure to raise "rubber-stamping" argument at trial is waiver).

3. Second, Agent Lawrence and the Digital Analyst reasonably believed that the Commanding Officer had a "substantial basis" to find probable cause.

Information presented to the magistrate cannot be "intentionally or recklessly false," and must be more than "bare bones." *Carter*, 54 M.J. at 421; *Leedy*, 65 M.J. at 212. The information "must contain sufficient information to permit the individual executing the warrant or authorization to reasonably believe

there is probable cause." *Carter*, 54 M.J. at 421. This prong examines the search authorization "through the eyes of a reasonable law enforcement official executing the search authorization," and is satisfied if "the law enforcement official had an objectively reasonable belief that the magistrate had a 'substantial basis' for determining the existence of probable cause." *Id.* at 422; *see Perkins*, 78 M.J. at 388.

Here, Agent Lawrence had an objectively reasonable belief that the Commanding Officer had a "substantial basis" for determining probable cause. Agent Lawrence presented the Commanding Officer with the Supporting Affidavit, which the Commander reviewed and signed, and the Military Judge found that two bases for probable cause were properly stated. (J.A. 394.)

Here, viewing the search authorization through the eyes of a "reasonable law enforcement official," it is apparent that there was an "objectively reasonable belief" that the Commanding Officer had a "substantial basis" to determine probable cause. *See Carter*, 54 M.J. at 420–22.

4. Third, Agent Lawrence and the Digital Analyst reasonably relied on the Command Authorization.

Officials may "reasonably and with good faith" rely on a search authorization unless: (1) they know that the magistrate "merely rubber stamped" their search request; or (2) when the warrant is "facially defective." *Carter*, 54

M.J. at 419. A warrant is facially defective where it fails "to particularize the place to be searched or the things to be seized." *Id.* at 419–21.

In *United States v. Christie*, 717 F.3d 1156, (10th Cir. 2013), the appellant challenged a warrant that authorized law enforcement to search a computer for "[a]ll records and information" relating to the murder, neglect, or abuse of a child. The *Christie* court found that, at bare minimum, an objectively reasonable officer acting in good faith could have read the warrant as restricting the scope of any search to information related to those specific crimes. *Id*. at 1166. Thus, the court declined to find that law enforcement should have known that the warrant was illegal despite the magistrate's authorization. *Id*.

Here, as in *Christie*, both Agent Lawrence and the Digital Analyst executing the Command Authorization "reasonably and with good faith" relied upon it. No evidence indicates that they believed the Commanding Officer "merely rubber stamped" the Command Authorization.

Nor did they know or believe it was "facially defective": no caselaw from this Court or others requires a specific listing of the applications within a phone that can be searched, and both this Court in *Richards* and other federal courts have approved similarly broad language. 76 M.J. at 370; *Smith*, 108 F. 4th at 879; *Corleto*, 56 F.4th 169. Because the good faith exception covers searches

conducted in objectively reasonable reliance on appellate precedent existing at the time of the search, it should apply here. *See Zodhiates*, 901 F. 3d at 143.

Moreover, law enforcement demonstrated their good faith reliance on the Command Authorization in the manner in which they conducted the search—they knew—and complied with—the parameters. The Digital Analyst reported that he followed the search parameters instructed by Agent Lawrence, which the Military Judge found was sufficiently particular because it matched the Affidavit. (J.A. 206, 400.)

Therefore, law enforcement's compliance with the Command Authorization demonstrates that they "reasonably and with good faith" relied on its issuance.

C. The lower court misapplied the "good faith" test, given that this Court in *Richards,* the Tenth Circuit, and most circuits reject particularity as to search locations *inside* digital devices.

The lower court rejects application of the good faith doctrine on the basis that the "authorization [is not] facially sufficient . . . [because] the CASS does not adequately specify . . . the location within the device as the Fourth Amendment requires." (J.A. 11.)[2] But that is not the law.

[2] Although the lower court's sentence in full reads "the device or the location," the lower court Opinion states in its particularity analysis that "for the purpose of this Article 62 review" the lower court does not rule on the particularity of the authorization as to *which devices* were to be seized: "Therefore, describing places to be searched under the general term 'digital devices' is far from particular. We concede the military judge took a different view of this issue and for the purpose of this Article 62 review do not further consider it." (J.A. 6.)

As demonstrated above, the lower court's view of the law is incorrect as to required particularity in warrants and authorizations as to locations *within* devices to be searched. Because the authorization was facially sufficient, the lower court should have found that good faith applied and precluded suppression of the evidence.

This is so because both the Special Agent and Digital Analyst seeking and executing the authorization reasonably relied on the authorization that—per *Richards* and the majority rule—permitted looking anywhere in the digital devices for evidence of listed specific crimes. *See* Mil. R. Evid. 311(c)(3); *United States v. Hernandez,* 81 M.J. 432, 440 (C.A.A.F. 2021); *Riccardi,* 405 F.3d at 864 ("the officers remained within the terms of the warrant as well as the affidavit, and did not conduct a 'fishing expedition' beyond the scope of the authorized investigation.").

D. The lower court misapplied *Carter* by failing to analyze the good faith exception as to the actions of digital analyst Mr. Soderquist in executing the Search Authorization.

In the lower court's analysis for good faith exception, it focused on Special Agent Lawrence and did not consider the digital analyst Mr. Soderquist. (J.A. 6). While Special Agent Lawrence applied for the Search Authorization, Mr. Soderquist searched Appellee's digital devices and found the incriminating evidence. (J.A. 206.)

This factual oversight renders the lower court's finding—that this case is unlike *United States v. Carter*, 54 M.J 414 (C.A.A.F. 2001)—incorrect. *See* (J.A. 11.). According to the lower court, "SA Lawrence prepared, presented and executed the CASS; in *Carter* a different agent presented the authorization than [sic] the agent who executed it." *Id.* (citing 54 M.J at 422). Because Mr. Soderquist searched the contents of Appellee's devices, while Special Agent Lawrence applied for the Search Authorization, the lower court erred in failing to apply *Carter*.

In *Carter*, the court found that the good faith exception applied because the executing agent reasonably believed that the requesting agent, who drafted an affidavit more than "bare bones," provided probable cause to the authorizing official. 54 M.J at 422.

Here, like *Carter*, Special Agent Lawrence's Supporting Affidavit to the Commanding Officer was more than "bare bones," as the lower court conceded. (J.A. 10.) Like *Carter*, it was thus objectively reasonable for Mr. Soderquist to believe that the Search Authorization was valid when searching Appellee's devices. *See* 54 M.J at 422.

The lower court erred in fact and law by failing to analyze Mr. Soderquist's actions and in misapplying binding precedent.

III.

ALTHOUGH INCORPORATION IS UNNECESSARY, THE MILITARY JUDGE ERRED WHEN HE FOUND THAT THE AUTHORIZATION DID NOT INCORPORATE THE PROBABLE CAUSE AFFIDAVIT. NOT ONLY DID THE AUTHORIZATION DIRECTLY REFERENCE THE "AFFIDAVITS BEING MADE BEFORE ME" BUT THE COMMANDING OFFICER SIGNED THE AUTHORIZATION AND THE AFFIDAVIT CONCURRENTLY. NONETHELESS, MIL R. EVID 315 REQUIRES ONLY THAT STATEMENTS BE COMMUNICATED TO AN AUTHORIZING OFFICIAL.

A. Standard of review.

The scope, applicability, and meaning of a statute are matters of statutory interpretation that are reviewed de novo. *United States v. Willman*, 81 M.J. 355, 357 (C.A.A.F. 2021).

B. Incorporation is not necessary here, where the Authorization was sufficiently particularized. The lower court and Military Judge erred finding that the Search Authorization did not already facially permit a search for everything listed in the Affidavit that was evidence of child pornography crimes.

The military judge's and lower court's misinterpretation of the required particularity for digital device searches renders incorporation under *Groh v. Ramirez*, 540 U.S. 551 (2004), unnecessary. No more particularity is needed for digital device searches for "evidence of" child pornography crimes to meet the

constitutional standard of particularity. (J.A. 405.) The Authorization itself here is sufficiently particular to search inside the devices for the evidence the Military Judge suppressed under *Richards* and current law. (J.A. 280.)

The Military Judge found that the "14 October 2022 NCIS Investigative Action" supported that "LtCol Cooley was provided a copy of the CASS and supporting [A]ffidavits for review," and referred to the "supporting [A]ffidavit" multiple times in his Findings. (J.A. 394.)

The Military Judge further found that Special Agent Lawrence "provided a list of the 'places' sought to be searched and the 'things' sought to be searched"—including digital storage devices, the Snapchat application, an email address, child pornography images and videos, proof of ownership of the devices, and applications where videos or photographs or records of them are stored. Yet the Military Judge went on to find "the actual CASS signed . . . does not include the[se] items . . . expressly or by reference." (J.A. 394–95.) The Military Judge then stated, "[l]ike *Groh* and *Armendariz*, the . . . probable cause statement within the CASS does not amount to sufficient words of incorporation." (J.A. 405.)

First, the Command Authorization for Search and Seizure states that law enforcement was authorized to search for "[e]vidence of . . . [p]ossession, receiving, or viewing of child pornography. . . and [d]istribution of [c]hild [p]ornography" in Appellee's "[d]igital devices." (J.A. 405.) Given, as

demonstrated above, that courts decline to impose *ex ante* search restrictions for the types of files or locations *within* digital devices that may be searched, the fact that the Affidavit is virtually identical to the text of the Search Authorization shows that no more particularity is needed and that the Authorization itself is sufficient. *See supra*, Section I.B.

Second, "Attachment A"—the Affidavit—provides a list that differs little from the Authorization in authorized scope: "devices capable of storing digital files . . . pertaining to . . . possessing, receiving, or viewing . . . [or d]istribution," a specific email address, images and videos relevant to those crimes, proof of ownership of the devices, and any applications where videos, photos, or records of either, might be stored. (J.A. 278; 280.) Further, the Military Judge erred finding that "Telegram" was not an application authorized to be searched—Telegram is unequivocally a place where evidence of possession, receipt, viewing, or distribution of child pornography can be found. (J.A. 405; *see infra* pp. 18–20.)

C. The Military Judge abused his discretion finding that the Supporting Affidavit was not incorporated into the Command Authorization, contrary to *Baranski* and *Richards*.

1. For affidavits to be incorporated into the warrant, the warrant must reference the affidavit and the affidavit must accompany the warrant.

Courts may "construe a warrant with reference to a supporting application or affidavit if the warrant uses appropriate words of incorporation, and if the

supporting document accompanies the warrant." *Groh v. Ramirez*, 540 U.S. 551, 557–58 (2004). Nonetheless, the warrant itself may still need to list the items to be seized. *See id.* at 554; *but see United States v. Bonner*, 808 F.2d 864 (1st Cir. 1986) (where address of residence to be searched was omitted from the warrant, but included in the affidavit, the warrant was still valid).

2. Like *Baranski*, the Command Authorization incorporated the Affidavit by express reference and the Commanding Officer's signature of both documents.

In *Baranski v. Fifteen Unknown Agents of the BATF*, 452 F.3d 433 (6th Cir. 2006), law enforcement applied for a warrant to search and seize "about 425 weapons" being held by the appellant at a warehouse. *Id*. at 436. The judge approved the warrant, relying on the affidavit that explained the appellant's scheme, detailed probable cause for the search, identified the places to be searched in the warehouse, and identified the machine guns to be seized. *Id*. The warrant itself did not identify the machine guns, but stated, "See Attached Affidavit." *Id*. The magistrate judge signed both the warrant and the affidavit. *Id*.

The *Baranski* court differentiated that case from *Groh*, where the warrant never cross-referenced the affidavit. *Id*. at 439–40. The court found that the warrant incorporated the affidavit because the magistrate judge signed both the warrant and affidavit, and the affidavit described with particularity the items to be seized. *Id*. at 440. Further, rather than a general authorization leaving the courts in

doubt whether "the [m]agistrate was aware of the scope of the search he was authorizing," this warrant authorized the seizure of 425 machine guns. *Id*. (distinguishing *Groh*, 540 U.S. at 561n.4). Unlike *Groh*, the warrant provided "written assurance that [he] actually found probable cause to search for, and to seize, every item mentioned in the affidavit." *Baranski*, 452 F.3d at 440 (quoting *Groh*, 540 U.S. at 560).

Here, like *Baranski*: (1) the Commanding Officer individually signed both the Search Authorization and Affidavit on the same day; (2) the Command Authorization referenced the "Affidavit(s) made before me" and "as stated in the supporting affidavit(s) "that provided the grounds for probable cause, and; (3) the Affidavit, as the Military Judge found, provided more details than the Search Authorization on the places in the phone to be searched and data to be seized because it specified that the targeted applications must be capable of storing photographs and videos. (J.A. 240–51, 268–80.)

3. Like *Richards*, the Affidavit guided the Command Authorization's particularity.

In *Richards*, the "affidavit accompanying the search request . . . detailed the investigation into [a]ppellant's relationship with [the minor victim], including the fact that the sexual relationship had been ongoing since approximately April 2011 with sexually explicit online communications starting about a year earlier." 76 M.J. at 367. In finding the search authorization "sufficiently particular," the court

noted "the authorization and accompanying affidavit did not give authorities carte blanche to search in areas clearly outside the scope of the crime being investigated." *Id.* at 370. Namely, law enforcement were "to search [a]ppellant's electronic media for any communication that related to his possible violation of the Florida statute in his relationship with [the minor victim]." *Id.*

Here, the Command Authorization here authorized the "search" and "seizure" of Appellee's "digital devices" for "[e]vidence of Article 134 (Possession, receiving, or viewing of child pornography) and Article 134 (Distribution of Child Pornography) of the [UCMJ]." (J.A. 280.) Like *Richards*, the Command Authorization had an Affidavit in Support which gave a more detailed description of "INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED." (J.A. 275–278); *see Richards*, 76 M.J. at 370.

Therein, Agent Lawrence requested authorization to "seize and search": "[a]ny and all computer, mobile or storage media devices capable of storing digital files" located in Appellee's barracks room and on his person, pertaining to his suspected possession and distribution of child pornography. (J.A. 268, 278.) Agent Lawrence also requested to search Appellee's seized devices for "Snapchat . . . ; Presence of [Appellee's] email address . . . ; Child pornography . . . ; Proof of ownership . . . ; [a]ny and all applications of which videos and photographs are stored or records thereof." (J.A. 278.) Agent

Lawrence requested permission to search Appellee's "cellular device, in any application or folders where photographs and videos may be stored." (J.A. 278.)

Thus, like *Richards*, the Command Authorization was also "sufficiently particular" when read with its accompanying Affidavit further describing what law enforcement sought to search and seize. *See Richards*, 76 M.J. at 370.

4. The Military Judge inaptly relied on *Groh* and *Armendariz*.

In *Groh*, the Supreme Court held that the warrant failed to identify the items law enforcement intended to seize and failed to incorporate the itemized list in the warrant application. 540 U.S. at 558. The warrant authorized "seizure" of a "single dwelling residence . . . blue in color." *Id*. That case did not address search or seizure of digital devices, and did not describe the targeted items—weapons, explosives, and records.

In *United States v. Armendariz*, 79 M.J. 535, 554 (N-M. Ct. Crim. App. 2019), *rev'd on other grounds*, 80 M.J. 130 (C.A.A.F. 2020), the court similarly held that the search authorization "did nothing to 'incorporate by reference' any language in the affidavit that might serve to limit the general search of the appellant's phones." 79 M.J. at 555 (citing *Groh*, 540 U.S. at 554–55). There, the search authorization did not limit search and seizure to evidence pertaining to the alleged misconduct. *Id.* at 554.

The Military Judge inaptly relied on *Groh* and *Armendariz*. (*See* J.A. 405.) Unlike *Groh* and *Armendariz*, the Command Authorization properly identified and limited the items to be searched and seized: "devices belonging to [Appellee]" and "[e]vidence of violations of Article 134 (Possession, receiving or viewing of child pornography) and Article 134 (Distribution of Child Pornography) of the Uniform Code of Military Justice." (J.A. 405.) It also expressly incorporated the Affidavit. (J.A. 405.) Further, like *Baranski* and unlike *Groh*, this is not a general "seizure" of a two-story blue house. Unlike both *Groh* and *Armendariz*, the Command Authorization here limited the search and seizure to evidence relating to child pornography, and only that which was located in digital devices belonging to Appellee. (J.A. 405.) This limitation was expressly understood by Agent Lawrence, who sought not to seize every conceivable digital device but to seize only those devices that were capable of storing child pornography. (J.A. 157.)

Therefore, the Command Authorization incorporated the Affidavit.

D. The lower court erred in declining to find that the Search Authorization incorporated the Affidavit.

The lower court declined to find the Affidavit incorporated where the Search Authorization first referred to "Affidavit(s) having been made before me by Special Agent [Lawrence]," and second referred to the Affidavit in what the lower court called "the boiler plate probable cause paragraph." (J.A. 8.) The lower court said that "the military judge found . . . that the affidavit did not accompany the

CASS." *Id.* The lower court said it "join[ed] the Eighth Circuit and the D.C. Circuit Court of Appeals" that "something more . . . than a boilerplate statement that the affidavit . . . constitute[s] probable cause" is required, and "agree[d] with the military judge that there was no actual incorporation." *Id.* at 10.

The lower court erred.

1. The lower court made factual and legal errors when it discounted the Affidavit for its boilerplate language, found the Affidavit's language only reference probable cause, and disregarded precedent finding cross-references sufficient.

First, nothing from the Supreme Court or this Court supports creating a rule that discounts the text of a search authorization—*signed by an appropriate authority*—because the language is "bold" or "boilerplate." Nor does anything support the lower court creating a rule that when the Authorization says that "grounds . . . for . . . a command authorization search exist *as stated in the supporting affidavit(s),*" that the Authorization does not incorporate that attached Affidavit. This Court should reject the lower court's rule that requires officials to "unbold" and re-type anew language from a form that they signed their name to as an official act in the military criminal justice system.

Second, the lower court errs in holding that the reference to the Affidavit was merely as to "probable cause"—the Authorization *first* ties the Affidavit to the conclusion that "I am satisfied that there is probable cause." (J.A. 280.) But

thereafter it states that "grounds for application for issuance of a command authorized search exist as stated in the supporting affidavit(s)." (J.A. 280.)

Third, the Supreme Court held that the particularity requirement may be satisfied through "express incorporation or *cross-referencing* of a supporting affidavit that describes the items to be seized." *Steagald v. United States*, 451 U.S. 204, 220 (1981) (emphasis added). In *Richards*, the Sixth Circuit found it was enough that the affidavit was cross-referenced in the application for the warrant. 659 F.3d at 533, 535 n.6. Like *Richards*, the Application by Special Agent Lawrence cross-referenced the Affidavit by including "See Attachment A." (J.A. 268.)

Fourth, the lower court erred given that the "Person Authorizing Search," like in *Baranski v. Fifteen Unknown Agents of the BATF*, 452 F.3d 433 (6th Cir. 2006)—the authorizing Commanding Officer himself—endorsed the Affidavit, which contained ten pages of facts supporting the application for a Search Authorization. (J.A. 279.) Despite that the same official authorizing the Search endorsing that eleven-page document, the lower court concluded it was not incorporated.

2. The lower court wrongly applies *Strand,* where the Eighth Circuit declined to incorporate an affidavit not signed by the judge that expanded the items to be searched for.

The lower court claimed that it joined the Eighth Circuit in *United States v. Strand*, 761 F.2d 449, 453 (8th Cir. 1985), given that the warrant in that case, like the Authorization here, merely referred to "Affidavit(s) having been made" and stated "grounds for application for issuance of a command authorized search exist as stated in the supporting affidavit(s)." (J.A. 8); *see Strand*, 761 F.2d at 453.

But the lower court wrongly applies that precedent because those facts are distinguishable from this case. The *Strand* warrant authorized postal inspectors to search for "stolen mail which is evidence of and the fruits of the crime of theft from the mail." *Strand*, 761 F.2d at 452–453. The *Strand* court declined to find that that warrant "permit[ed] the seizure of items which do not fit into the . . . category" of "stolen mail," including "many . . . items seized . . . not found in parcels of mail, . . . includ[ing] items such as socks, a sweatshirt, cosmetics, a sweater, a thermometer, a china plate, and gloves." *Id.* The *Strand* court found that "a warrant commanding postal inspectors to seize 'stolen mail' clearly does not authorize them to seize items ordinarily considered to be normal household goods." *Id.* The *Strand* court did not find incorporation with language almost identical to this case, but there, unlike the case here and *Baranski*, the magistrate

had not endorsed the affidavit providing additional items to be seized. The lower court erred factually and legally.

3. The lower court erroneously crafts a *per se* rule that rejects the use of boilerplate. The Eighth Circuit in *Johnson*—cited in *Strand*— found incorporation where the warrant said "as described in the affidavit"—like "as stated in" in this case. And *Baranski* turned on the magistrate's "signing" of the affidavit—like the Authorizing Official's signature on the Affidavit here. This Court should find incorporation.

Strand cited to *United States v. Johnson*, 541 F.2d 1311 (8th Cir. 1976), where the Eighth Circuit did find incorporation, and the lower court missed that this case is like *Johnson*. The *Johnson* warrant authorized seizure of "marijuana, parphenrnalia [sic] and U.S. currency *as described in* the affidavit," and the search resulted in seizure of "four twenty-dollar bills having serial numbers listed in the affidavit." 541 F.2d at1313 (emphasis added). The *Johnson* court noted that "it is clear that the language of the warrant was . . . narrowed by its reference to the affidavit and . . . sufficiently definite to meet the constitutional standard of particularity." *Id.* at 1316.

First, the lower court misses that while *Strand* rejected incorporation, *Johnson permitted* incorporation, where the "as described in the affidavit" language there is close to the "as stated in" language in the Affidavit here. *Johnson,* 541 F.2d at 1313; (J.A. 280). Second, the lower court appears to miss that *Baranski*'s finding of incorporation turns not on the language of "specific"

incorporation but on the fact that the magistrate specifically signed the attached affidavit, which the court cited numerous times as a distinguishing fact from *Groh*. *Baranski*, 452 F.3d at 440, 444 ("this warrant and affidavit (*and the magistrate's signature on both* of them) made it clear that the magistrate found that there was probable cause to support the search" and "[*Groh*] might well have been different if the facially defective warrant had been attached to an affidavit signed by the magistrate") (emphasis added).

Where the Authorizing Official specifically endorsed the Affidavit, adding granularity to the evidence supporting the crimes of possessing, distributing, and viewing child pornography, this Court should first find that no further particularity was constitutionally required beyond the Authorization, and second, even if it was, this case is more like *Johnson*, *Baranski*, and *Richards* given that the authorizing Commanding Officer signed the Affidavit, and the Authorization and Application properly incorporated the Affidavit by reference.

E. Nonetheless, "appropriate words of incorporation" are not required for for a court to construe an authorization using an affidavit.

The President promulgated Mil. R. Evid. 315 to specify what to consider in evaluating probable cause. Specifically, probable cause "will" be based upon written or oral statements made to an authorizing official. Mil R. Evid. 315(f).

In *Perkins*, law enforcement called the commanding officer and requested permission to search the appellant's effects; they explained the residence, where it

was located, and the facts of the allegation. 78 M.J. at 384. The commanding officer granted permission, also telephonically, without a written authorization. *Id*. This Court, without deciding whether there was sufficient basis for probable cause, found that law enforcement relied on the authorization in good faith. *Id*. at 389.

Here, the basis for probable cause was communicated to the Commanding Officer; he acknowledged as much from his signature. (J.A. 279–80.) The Military Judge's use of *Groh* in determining that the authorization was not incorporated was incorrect because—distinct from a warrant—a search authorization can be valid even where the information supporting probable cause has been communicated telephonically, and where the permission has been granted telephonically. Thus, as here, where the sworn Affidavit was presented in writing, the authorization was granted in writing, and the commander signed both documents contemporaneously, this Court should construe the authorization with respect to the Affidavit. Nonetheless, as argued above, incorporation of the Affidavit was unnecessary, as the Authorization specified the suspected offenses and directed the search be limited to evidence of those specific offenses. *See supra*, Section I.

IV.

THE EXCLUSIONARY RULE SHOULD NOT APPLY BECAUSE SUPPRESSING THE EVIDENCE WOULD HAVE LITTLE TO NO DETERRENT EFFECT AND DOES NOT OUTWEIGH THE COSTS TO THE JUSTICE SYSTEM.

A. Standard of review.

This Court reviews a military judge's ruling on suppression's deterrent effect and whether such deterrence outweighs the costs to the justice system to determine whether the judge's assessment of these matters was a "clearly unreasonable" exercise of discretion. *United States. v. Lattin*, 83 M.J. 192, 198 (C.A.A.F. 2023).

B. The exclusionary rule applies where suppression of evidence would have an appreciable deterrent effect on Fourth Amendment violations and outweigh any harm to the justice system.

The military implements the protections of the Fourth Amendment through Mil. R. Evid. 311–317. *United States v. Hoffman*, 75 M.J. 120, 123 (C.A.A.F. 2016). Those rules are intended to "express the manner in which the Fourth Amendment to the Constitution of the United States applies to trials by court-martial." Manual for Courts-Martial, United States, Analysis of the Military Rules of Evidence app. 22 at A22-17 (2012 ed.).

The exclusionary rule is a "judicially created remedy for violations of the Fourth Amendment." *United States v. Wicks*, 73 M.J. 93, 103 (C.A.A.F. 2014).

The regulatory implementation of the exclusionary rule in the Military Rules of Evidence generally prohibits admission of evidence obtained as a result of an unlawful search or seizure. Mil. R. Evid. 311(a). It is "designed to safeguard Fourth Amendment rights generally through its deterrent effect, rather than a personal constitutional right of the party aggrieved." *United States v. Leon*, 468 U.S. 897, 906 (1984); *see also Davis v. United States*, 564 U.S. 229, 236–37 (2011) (Court has "repeatedly held" that exclusionary rule's "sole purpose . . . is to deter future Fourth Amendment violations").

The exclusionary rule was "adopted to deter unlawful searches by police, not to punish the errors of magistrates and judges." *Massachusetts v. Shepard*, 468 U.S. 981, 990 (1984) (internal quotations omitted); *Davis*, 564 U.S. at 238–39 ("punishing the errors of judges is not the office of the exclusionary rule") (internal quotations and citations omitted).

To warrant exclusion, "police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Herring v. United States*, 555 U.S. 135, 144 (2009). When police conduct "involves only simple, 'isolated' negligence . . . the 'deterrence rationale loses much of its force,' and exclusion cannot 'pay its way.'" *Davis*, 564 U.S. at 238–39 (internal quotations and citations omitted). Exclusion is therefore unwarranted where police negligence is "isolated"

or "nonrecurring." *Davis*, 564 U.S. at 239 (citing *Herring*, 555 U.S. at 137, 144). Society must swallow the "bitter pill" of exclusion as a last resort. *Id.* at 237.

Therefore, the exclusionary rule "does not apply every time law enforcement officials violate the Fourth Amendment." *United States v. Lattin*, 83 M.J. 192, 197 (C.A.A.F. 2023). The standing rule has been to limit exclusion "to cases in which the prosecution seeks to use the fruits of an illegal search or seizure against the victim of police misconduct." *Leon*, 468 U.S. at 916. "This is particularly true, we believe, when an officer acting with objective good faith has obtained a search warrant from a judge or magistrate and acted within its scope." *Id*. at 920.

This is consistent with the President's codification of the exclusionary rule: "Evidence obtained as a result of an unlawful search or seizure made by a person acting in a governmental capacity is inadmissible against the accused if . . . exclusion of the evidence results in appreciable deterrence of future unlawful searches or seizures and the benefits of such deterrence outweigh the costs to the justice system." Mil. R. Evid. 311(a).

2. Like *Lattin*, the exclusionary rule would serve no deterrent effect here and would be "substantial" cost to the justice system.

In *United States v. Lattin*, No. 39859, 2022 CCA LEXIS 226 (A.F. Ct. Crim. App. Apr. 20, 2022), *aff'd*, 83 M.J. 192 (C.A.A.F. 2023), the court held that the warrant to search a mobile device was improperly broad because it failed to

identify the data to be seized. *Id*. at *36–37. Nonetheless, exclusion was not warranted because the court did not find (1) appreciable deterrence of future unlawful search or seizures and (2) that benefits of such deterrence outweigh the costs to the justice system. *Id*. at *45. The court did not find that the military judge erred in holding that: (1) law enforcement acted reasonably considering the nature of digital evidence; (2) law enforcement did not violate appellant's Fourth Amendment rights deliberately, recklessly, or with gross negligence; and (3) the violation was an accident and not by design. *Id*. at *50; *see Herring*, 555 U.S. at 144. That court considered any deterrent value to be speculative, contrasted with high costs to justice system. *Lattin*, 2022 CCA LEXIS 226, at *53–54. The appellant was charged of sexual assault and abusive sexual contact against two victims. *Id*. at *54.

Like *Lattin*, any deterrence of future unlawful search or seizures would at best would be speculative. Even if law enforcement violated the Fourth Amendment, they explained the process complications with digital evidence in the Affidavit and neither the Record, Agent Lawrence's testimony, nor the Military Judge's findings indicate that such violation was deliberate, reckless, or grossly negligent. (J.A. 142–174, 242–246, 408–409.); s*ee Herring*, 555 U.S. at 144. The Military Judge's reasoning that suppression would incentivize commanding officers and law enforcement to include more search parameters in the CASS itself,

rather than in an Affidavit, ignores that no other court has recognized that incentive as a valid justification for deterrence. This conclusion ignores that the focus of the exclusionary rule is law enforcement, not magistrates. *See United States v. McLamb*, 880 F. 3d 685, 691 (4th Cir. 2018) (citing *United States v. Leon*, 468 U.S. 897, 916 (1984)). Further, the military judge did not identify any cases law enforcement could have relied on to understand their CASS was invalid. *See Zodhiates*, 901 F. 3d at 143; J.A. 408–409.

In contrast to the Military Judge's speculation as to deterrence, his conclusion that the cost of excluding the evidence would be "substantial" was based on significant evidence. (J.A. 409.) Appellee is charged with possession, receiving, distribution, and soliciting distribution of child pornography. (J.A. 136–141.) Appellee's conduct victimized countless minor children, considering 254 video files and 272 picture files in Appellee's iPhone were potentially child pornography. (J.A. 206.) The Military Judge was also aware that suppressing the contents of the phone would likewise completely prevent the United States from presenting Appellee's text messages exhibiting his distribution and solicitation thereof, which demonstrated that Appellee was attempting to trade potential child pornography in exchange for "rape vids" involving "incest and younger boys." (J.A. 212.)

Therefore, in balancing the "substantial" costs to the justice system with the speculative value of deterrence, the digital evidence seized from Appellee's iPhone should not be excluded. The Military Judge erred.

3. The lower court relied on the Military Judge's incorrect application of law that Mr. Soderquist exceeded Special Agent Lawrence's directive. This Court should not apply the exclusionary rule.

The lower court found appreciable deterrence in its exclusionary rule analysis because "[t]herein the military judge noted that DC3 seized information beyond the scope of SA Lawrence's request based on its facially broad authorization." (J.A. 14.)

But the Military Judge's note was incorrect and the lower court relies on an error. Special Agent Lawrence asked Mr. Soderquist to "recover and analy[ze] the following items:

> Identify items pertaining to the suspected violations of Article 134 [Possessing, receiving, or viewing Child Sexual Abuse Material (CSAM)] and Article 134 (Distribution of Child Pornography) of the Uniform Code of Military Justice (UCMJ).
>
> Snapchat messaging application pertaining to the above mentioned violations of the UCMJ.
>
> Presence of the email address [email address omitted].
>
> Proof of ownership of the submitted evidence items.
>
> Any and all applications in which videos and/or photographs are stored or records of.

(J.A. 206).

According to the Military Judge, Mr. Soderquist exceeded Special Agent Lawrence's request by seizing the Telegram messages in Appellee's phone. (J.A. 405.)

But the Military Judge's application of law is rejected by *United States v. Shields*, 83 M.J. 226 (C.A.A.F. 2023), where the court gave deference to the expertise and methodology of digital analysts to search for child pornography in digital devices. *Id*. at 234. Here, the search of Telegram reasonably falls within Special Agent Lawrence's request, constituting search of "any and all applications" where "videos and/or photographs are stored or records of." (J.A. 206.) The Military Judge even acknowledged that two CSAM images were found in Appellee's Telegram application. (J.A. 396.) Like in *Shields*, where the analyst properly seized child pornography while only authorized to search for "location data," the plain view doctrine applies when the digital search was lawful. 83 M.J. at 235. The Telegram messages were lawfully seized.

The Military Judge clearly misunderstood and misapplied the law governing the scope of searches inside digital devices. The lower court adopts that misunderstanding, as demonstrated by its misunderstanding as to the constitutionally required particularity for search authorizations inside digital

devices. This Court should reject that interpretation of the law, apply *Shields*, and find that exclusion is not appropriate.

Conclusion

The United States respectfully requests this Court vacate the Military Judge's Ruling, reverse the lower court's Opinion, find the evidence acquired under the Command Authorization admissible, and remand for further proceedings.

JACOB R. CARMIN
Captain, U.S. Marine Corps
Appellate Government Counsel
Navy-Marine Corps Appellate
Review Activity
Bldg. 58, Suite B01
1254 Charles Morris Street SE
Washington Navy Yard, DC 20374
(202) 685-4623, fax (202) 685-7687
Bar no. 37530

MARY CLAIRE FINNEN
Major, U.S. Marine Corps
Senior Appellate Counsel
Navy-Marine Corps Appellate
Review Activity
Bldg. 58, Suite B01
1254 Charles Morris Street SE
Washington Navy Yard, DC 20374
(202) 685-7686, fax (202) 685-7687
Bar no. 37338

IAIN D. PEDDEN
Colonel, U.S. Marine Corps
Director, Appellate Government
Navy-Marine Corps Appellate
Review Activity
Bldg. 58, Suite B01
1254 Charles Morris Street SE
Washington Navy Yard, DC 20374
(202) 685-7427, fax (202) 685-7687
Bar no. 33211

BRIAN K. KELLER
Deputy Director
Appellate Government
Navy-Marine Corps Appellate
Review Activity
Bldg. 58, Suite B01
1254 Charles Morris Street SE
Washington Navy Yard, DC 20374
(202) 685-7682, fax (202) 685-7687
Bar no. 31714

Certificate of Compliance

1. This brief complies with the type-volume limitation of Rule 24(b) because this brief contains 12,981 words.

2. This brief complies with the typeface and type style requirements of Rule 37 because this brief was prepared in a proportional typeface using Microsoft Word with 14-point Times New Roman font.

Certificate of Filing and Service

I certify this document was emailed to the Court's filing address, uploaded to the Court's case management system, and emailed to Appellate Defense Counsel Lieutenant Meggie KANE-CRUZ, JAGC, U.S. Navy, on September 18, 2025.

JACOB R. CARMIN
Captain, U.S. Marine Corps
Senior Appellate Counsel

Appendix A

Rule 311. Evidence obtained from unlawful searches and seizures

(a) *General rule*. Evidence obtained as a result of an unlawful search or seizure made by a person acting in a governmental capacity is inadmissible against the accused if:

(1) the accused makes a timely motion to suppress or an objection to the evidence under this rule;

(2) the accused had a reasonable expectation of privacy in the person, place, or property searched; the accused had a legitimate interest in the property or evidence seized when challenging a seizure; or the accused would otherwise have grounds to object to the search or seizure under the Constitution of the United States as applied to members of the Armed Forces; and

(3) exclusion of the evidence results in appreciable deterrence of future unlawful searches or seizures and the benefits of such deterrence outweigh the costs to the justice system.

(b) *Definition*. As used in this rule, a search or seizure is "unlawful" if it was conducted, instigated, or participated in by:

(1) military personnel or their agents and was in violation of the Constitution of the United States as applied to members of the Armed Forces, a federal statute applicable to trials by court-martial that requires exclusion of evidence obtained in violation thereof, or Mil. R. Evid. 312-317;

(2) other officials or agents of the United States, of the District of Columbia, or of a State, Commonwealth, or possession of the United States or any political subdivision of such a State, Commonwealth, or possession, and was in violation of the Constitution of the United States, or is unlawful under the principles of law generally applied in the trial of criminal cases in the United States district courts involving a similar search or seizure; or

(3) officials of a foreign government or their agents, where evidence was obtained as a result of a foreign search or seizure that subjected the accused to gross and brutal maltreatment. A search or seizure is not "participated in" by a United States military or civilian official merely because that person is present at a search or seizure conducted in a foreign nation by officials of a foreign government or their agents, or because that person acted as an interpreter or took steps to mitigate damage to property or physical harm during the foreign search or seizure.

(c) *Exceptions*.

(1) *Impeachment*. Evidence that was obtained as a result of an unlawful search or seizure may be used to impeach by contradiction the in-court testimony of the accused.

(2) *Inevitable Discovery*. Evidence that was obtained as a result of an unlawful search or seizure may be used when the evidence would have been obtained even if such unlawful search or seizure had not been made.

(3) *Good Faith Exception of a Warrant or Search Authorization*: Evidence that was obtained as a result of an unlawful search or seizure may be used if:

(A) the search or seizure resulted from an authorization to search, seize, or apprehend issued by an individual competent to issue the authorization under Mil. R. Evid. 315(d) or from a search warrant or arrest warrant issued by competent civilian authority, or from such an authorization or warrant issued by an individual whom the officials seeking and executing the authorization or warrant reasonably and with good faith believed was competent to issue the authorization or warrant;

(B) the individual issuing the authorization or warrant had a substantial basis for determining the existence of probable cause or the officials seeking and executing the authorization or warrant reasonably and with good faith believed that the individual issuing the authorization or warrant had a substantial basis for determining the existence of probable cause; and

(C) the officials seeking and executing the authorization or warrant reasonably and with good faith relied on the issuance of the authorization or warrant. Good faith is to be determined using an objective standard.

(4) *Reliance on Statute or Binding Precedent*.

Evidence that was obtained as a result of an unlawful search or seizure may be used when the official seeking the evidence acted in objectively reasonable reliance on a statute or on binding precedent later held violative of the Fourth Amendment.

(d) *Motions to Suppress and Objections*.

(1) *Disclosure*. Prior to arraignment, the prosecution must disclose to the defense all evidence seized from the person or property of the accused, or believed to be owned by the accused, or evidence derived therefrom, that it intends to offer into evidence against the accused at trial.

(2) *Time Requirements*.

(A) When evidence has been disclosed prior to arraignment under subdivision (d)(1), the defense must make any motion to suppress or objection under this rule prior to submission of a plea. In the absence of such motion or objection, the defense may not raise the issue at a later time except as permitted by the military

judge for good cause shown. Failure to so move or object constitutes a waiver of the motion or objection.

(B) If the prosecution intends to offer evidence described in subdivision (d)(1) that was not disclosed prior to arraignment, the prosecution must provide timely notice to the military judge and to counsel for the accused. The defense may enter an objection at that time and the military judge may make such orders as are required in the interest of justice.

(3) *Specificity*. The military judge may require the defense to specify the grounds upon which the defense moves to suppress or object to evidence described in subdivision (d)(1). If defense counsel, despite the exercise of due diligence, has been unable to interview adequately those persons involved in the search or seizure, the military judge may enter any order required by the interests of justice, including authorization for the defense to make a general motion to suppress or a general objection.

(4) *Challenging Probable Cause*.

(A) *Relevant Evidence*. If the defense challenges evidence seized pursuant to a search warrant or search authorization on the ground that the warrant or authorization was not based upon probable cause, the evidence relevant to the motion is limited to evidence concerning the information actually presented to or otherwise known by the authorizing officer, except as provided in subdivision (d)(4)(B).

(B) *False Statements*. If the defense makes a substantial preliminary showing that a government agent knowingly and intentionally or with reckless disregard for the truth included a false statement or omitted a material fact in the information presented to the authorizing officer, and if the allegedly false statement or omitted material fact is necessary to the finding of probable cause, the defense, upon request, is entitled to a hearing. At the hearing, the defense has the burden of establishing by a preponderance of the evidence the allegation of knowing and intentional falsity or reckless disregard for the truth. If the defense meets its burden, the prosecution has the burden of proving by a preponderance of the evidence, with the

false information set aside, that the remaining information presented to the authorizing officer is sufficient to establish probable cause. If the prosecution does not meet its burden, the objection or motion must be granted unless the search is otherwise lawful under these rules."

(5) *Burden and Standard of Proof*.

(A) *In general*. When the defense makes an appropriate motion or objection under subdivision (d), the prosecution has the burden of proving by a preponderance of the evidence that the evidence was not obtained as a result of an unlawful search or seizure; that the evidence would have been obtained even if the unlawful search or seizure had not been made; that the evidence was obtained by officials who reasonably and with good faith relied on the issuance of an authorization to search, seize, or apprehend or a search warrant or an arrest warrant; that the evidence was obtained by officials in objectively reasonable reliance on a statute or on binding precedent later held violative of the Fourth Amendment; or that the deterrence of future unlawful searches or seizures is not appreciable or such deterrence does not outweighthe costs to the justice system of excluding the evidence.

(B) *Statement Following Apprehension*. In addition to subdivision (d)(5)(A), a statement obtained from a person apprehended in a dwelling in violation of R.C.M. 302(d)(2) and (e), is admissible if the prosecution shows by a preponderance of the evidence that the apprehension was based on probable cause, the statement was made at a location outside the dwelling subsequent to the apprehension, and the statement was otherwise in compliance with these rules.

(C) *Specific Grounds of Motion or Objection*. When the military judge has required the defense to make a specific motion or objection under subdivision (d)(3), the burden on the prosecution extends only to the grounds upon which the defense moved to suppress or objected to the evidence.

(6) *Defense Evidence*. The defense may present evidence relevant to the admissibility of evidence as to which there has been an appropriate motion or objection under this rule. An accused may testify for the limited purpose of contesting the legality of the search or seizure giving rise to the challenged evidence. Prior to the introduction of such testimony by the accused, the defense must inform the military judge that the testimony is offered under subdivision (d). When the accused testifies under subdivision (d), the accused may be cross-examined only as to the matter on which he or she testifies. Nothing said by the accused on either direct or cross-examination may be used against the accused for any purpose other than in a prosecution for perjury, false swearing, or the making of a false official statement.

(7) *Rulings*. The military judge must rule, prior to plea, upon any motion to suppress or objection to evidence made prior to plea unless, for good cause, the military judge orders that the ruling be deferred for determination at trial or after findings. The military judge may not defer ruling if doing so adversely affects a party's right to appeal the ruling. The military judge must state essential findings of fact on the record when the ruling involves factual issues.

(8) *Informing the Members*. If a defense motion or objection under this rule is sustained in whole or in part, the court-martial members may not be informed of that fact except when the military judge must instruct the members to disregard evidence.

(e) *Effect of Guilty Plea*. Except as otherwise expressly provided in R.C.M. 910(a)(2), a plea of guilty to an offense that results in a finding of guilty waives all issues under the Fourth Amendment to the Constitution of the United States and Mil. R. Evid. 311-317 with respect to the offense, whether or not raised prior to plea.

Rule 315. Probable cause searches

(a) *General rule*. Evidence obtained from reasonable searches conducted pursuant to a search warrant or search authorization, or under the exigent circumstances described in this rule, is admissible at trial when relevant and not otherwise inadmissible under these rules or the Constitution of the United States as applied to members of the Armed Forces.

(b) *Definitions*. As used in these rules:

(1) "Search authorization" means express permission, written or oral, issued by competent military authority to search a person or an area for specified property or evidence or for a specific person and to seize such property, evidence, or person. It may contain an order directing subordinate personnel to conduct a search in a specified manner.

(2) "Search warrant" means express permission to search and seize issued by competent civilian authority or under R.C.M. 703A.

(3) "Warrant for wire or electronic communications" means a warrant issued by a military judge pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A), or (c)(1)(A) in accordance with 10 U.S.C. § 846(d)(3) and R.C.M. 309(b)(2) and R.C.M. 703A.

(c) *Scope of Search Authorization*. A search authorization may be valid under this rule for a search of:

(1) the physical person of anyone subject to military law or the law of war wherever found;

(2) military property of the United States or of nonappropriated fund activities of an Armed force of the United States wherever located;

(3) persons or property situated on or in a military installation, encampment, vessel, aircraft, vehicle, or any other location under military control, wherever located; or

(4) nonmilitary property within a foreign country.

(d) *Who May Authorize*. A search authorization under this rule is valid only if issued by an impartial individual in one of the categories set forth inparagraphs (d)(1), (d)(2), and (d)(3) of

this rule. Only a military judge may issue a warrant for wire or electronic communications under this rule. An otherwise impartial authorizing official does not lose impartiality merely because the official is present at the scene of a search or is otherwise readily available to persons who may seek the issuance of a search authorization; nor does such an official lose impartial character merely because the official previously and impartially authorized investigative activities when such previous authorization is similar in intent or function to a pretrial authorization made by the United States district courts.

(1) *Commander*. A commander or other person serving in a position designated by the Secretary concerned as either a position analogous to an officer in charge or a position of command, who has control over the place where the property or person to be searched is situated or found, or, if that place is not under military control, having control over persons subject to military law or the law of war;

(2) *Military Judge or Magistrate*. A military judge or magistrate if authorized under regulations prescribed by the Secretary of Defense or the Secretary concerned; or

(3) *Other competent search authority*. A competent, impartial official as designated under regulations by the Secretary of Defense or the Secretary concerned as an individual authorized to issue search authorizations under this rule.

(e) *Who May Search*.

(1) *Search Authorization*. Any commissioned officer, warrant officer, petty officer, noncommissioned officer, and, when in the execution of guard or police duties, any criminal investigator, member of the Air Force security forces, military police, or shore patrol, or person designated by proper authority to perform guard or police duties, or any agent of any such person, may conduct or authorize a search when a search authorization has been granted under this rule or a search would otherwise be proper under subdivision (g).

(2) *Search Warrants*. Any civilian or military criminal investigator authorized to request search warrants pursuant to applicable law or regulation is authorized to serve and execute search warrants. The execution of a search warrant affects admissibility only insofar as exclusion of evidence is required by the Constitution of the United States or an applicable federal statute.

(f) *Basis for Search Authorizations*.

(1) *Probable Cause Requirement*. A search authorization issued under this rule must be based upon probable cause.

(2) *Probable Cause Determination*. Probable cause to search exists when there is a reasonable belief that the person, property, or evidence sought is located in the place or on the person to be searched. A search authorization may be based upon hearsay evidence

in whole or in part. A determination of probable cause under this rule will be based upon any or all of the following:

(A) written statements communicated to the authorizing official;

(B) oral statements communicated to the authorizing official in person, via telephone, or by other appropriate means of communication; or

(C) such information as may be known by the authorizing official that would not preclude the officer from acting in an impartial fashion. The Secretary of Defense or the Secretary concerned may prescribe additional requirements through regulation.

(g) *Exigencies*. Evidence obtained from a probable cause search is admissible without a search warrant or search authorization when there is a reasonable belief that the delay necessary to obtain a search warrant or search authorization would result in the removal, destruction, or concealment of the property or evidence sought. Military operational necessity may create an exigency by prohibiting or preventing communication with a person empowered to grant a search authorization.