

*How to Use the Privacy Act to Access an Army Adverse Information Program (AAIP)
Portal Entry: A Guide to Seeing Your Records***

A lack of transparency results in distrust and a deep sense of insecurity.¹

I. Introduction

In April 2023, Captain (CPT) Smith learned he was the subject of an Army Regulation (AR) 15-6 administrative investigation into allegations that he engaged in an extramarital, adulterous relationship.² At the advice of expensive, privately-hired counsel he invoked his rights—understanding he would have an opportunity to review and rebut any potential

* Major Whitney Wiles is a Judge Advocate in the United States Army presently assigned to the Litigation Division within the United States Army Legal Services Agency. Major Wiles received an LL.M. in federal litigation from University of Virginia School of Law in 2023; an LL.M. in military law from The Judge Advocate General's School in 2021; a J.D. from Florida Coastal in 2011; and a B.S. in Journalism from Ohio University in 2007. Her previous assignments include: Associate Professor in the Administrative and Civil Law Department at The Judge Advocate General's School where she taught Investigations, the Army Adverse Information Program, Sexual Harassment, and Equal Opportunity; Officer-in-Charge of the Kleber Legal Services Center and Rheinland-Pfalz Garrison Legal Advisor, U.S. Army Garrison, Kaiserslautern, Germany; Deputy Chief of Administrative and Civil Law, 21st Theater Sustainment Command, Kaiserslautern, Germany; Senior Defense Counsel, Trial Defense Service, Fort Leonard Wood, Missouri; Prosecutor, 3rd Brigade Combat Team, 25th Infantry Division, Schofield Barracks, Hawaii; Administrative Law Attorney, 25th Infantry Division, Schofield Barracks, Hawaii; Tax Center Officer-in-Charge, U.S. Army Garrison, Schofield Barracks, Hawaii; and Legal Assistance Attorney, U.S. Army Garrison, Schofield Barracks, Hawaii. Major Wiles is a member of the Bars of Illinois, the Army Court of Criminal Appeals, the United States Court of Appeals for the Armed Forces, and the United States Supreme Court.

* Major Retland is a Judge Advocate in the United States Army presently serving as the Assistant Executive Officer at The Judge Advocate General's Legal Center and School. He received his B.A. in Criminal Justice from The Citadel in 2008, his J.D., *cum laude*, from Michigan State University College of Law in 2012 and an LL.M. from The Judge Advocate General's School. His previous assignments include: Associate Professor in the Administrative and Civil Law Department at The Judge Advocate General's School where he taught Government Information Practice; Special Victims' Counsel Central Region Manager, III Corps, Fort Cavazos, Texas; National Security Law Attorney, Combined Joint Task Force-Operation Inherent Resolve, Baghdad, Iraq; Brigade Judge Advocate, 48th Chemical Brigade, III Corps, Fort Cavazos, Texas; Chief of Military Justice and Administrative Law, United States Military Entrance Processing Command, Great Lakes, Illinois; Trial Counsel, United States Army Central Command, Shaw Air Force Base, South Carolina. Major Retland is a member of the bars of Michigan, the District of Columbia, and the United States Supreme Court.

¹ Dalai Lama.

² U.S. DEP'T OF ARMY, REG. 15-6, Procedures for Administrative Investigations and Boards of Officers (1 Apr. 2016) [hereinafter AR 15-6].

adverse findings made against him before the investigation was fully closed.³ Upon completion of the investigation, the approval authority referred the adverse portions of the investigation to CPT Smith for rebuttal and advised him that if the contemplated, adverse finding—a finding that he engaged in an inappropriate (but not adulterous) relationship—was ultimately approved, the finding would be presented directly to his O-4 promotion selection board (PSB) for consideration on whether he should be recommended for promotion to the rank of Major.⁴ What was not made entirely clear to CPT Smith in his referral memorandum was that any approved, adverse findings would be summarized and uploaded, along with other personally identifiable information (PII) relating to him, into the Army Adverse Information Program (AAIP) database.⁵ Based on CPT Smith’s date of rank, his O-4 PSB would not meet for at least six years.⁶

In his rebuttal, CPT Smith argued, through counsel, that the relationship at issue was not inappropriate and—even if the approval authority disagreed—the proposed finding was not

³ U.S. DEP’T OF ARMY, DIR. 2023-03, ARMY ADVERSE INFORMATION PROGRAM (22 Feb. 2023) [hereinafter AD 2023-03].

⁴ 10 U.S.C. §§ 615, 14107; U.S. DEP’T OF ARMY, REG. 600-8-29, OFFICER PROMOTIONS (9 Sep. 2020) [hereinafter AR 600-8-29] (documenting that active duty promotions to the rank of Major and higher must be confirmed by the Senate); U.S. DEP’T OF DEF., INSTR 1320.04, MILITARY OFFICER ACTIONS REQUIRING PRESIDENTIAL, SECRETARY OF DEFENSE, OR UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS APPROVAL OR SENATE CONFIRMATION, encl 6 (3 Jan. 2014) (C1, 30 Jun. 2020) [hereinafter DoDI 1320.04] (detailing that Senate confirmation is also required for O-6 Reserve Component nominations); ARMY ADVERSE INFORMATION PROGRAM (AAIP) USER GUIDE V. 2.0 AT 6, 12 (Mar. 2023) [hereinafter AAIP USER GUIDE] (including a new referral of report of investigation, which notifies both company and field grade officers that adverse information must be furnished to a promotion selection board); AR 15-6 *supra* note 2 at para. 2-8c (outlining rebuttal rights). Of note, AR 15-6 rebuttal rights only guarantee access to the “adverse” portions of the investigation as determined by the legal advisor and do not guarantee access to the investigation in its entirety. AR 15-6, para. 2-8; *see infra* n. 36.

⁵ Interestingly, the template referral memorandum in the AAIP User Guide does not reference the Army Adverse Information Program (AAIP) database at all. AAIP USER GUIDE at 6. Unrepresented respondents may not even be aware that the AAIP database exists or understand where the adverse finding(s) will be stored until such time as their promotion board, or another Department of the Army (DA) selection board convenes. *See id.*

⁶ *See* Personnel, Plans, and Training Office, FY23 – FY27 JAGC AC MAJ Promotion Selection Board Primary Zone Forecast (Feb. 24, 2023) *available at* <https://www.jagcnet2.army.mil/>.

“adverse” per the definition in Department of Defense Instruction (DoDI) 1320.04 and replicated in AR 15-6.⁷ After timely submitting his matters—from his perspective—nothing happened: CPT Smith was not counseled or reprimanded and he received no punitive action. Captain Smith moves on with his life. He makes career decisions, which align with a military retirement. However, in 2029, six years after the investigation, CPT Smith receives a surprising notification from Human Resources Command (HRC) advising him that he has adverse information in his O-4 PSB “My Board File.”⁸ Only at this point does HRC provide CPT Smith with the opportunity to review the specifics of the summarized adverse entry in his file and the chance to submit a comment to the promotion board regarding the adverse information.⁹ Upon review, CPT Smith disagrees with the summarized adverse finding that the Office of the Staff Judge Advocate (OSJA) uploaded into the AAIP database. However,

⁷ AR 15-6 *supra* note 2 at Section II Terms (“Adverse information is any substantiated adverse finding or conclusion from an officially documented investigation or inquiry or any other credible information of an adverse nature. To be credible, the information must be resolved and supported by a preponderance of the evidence. To be adverse, the information must be derogatory, unfavorable, or of a nature that reflects clearly unacceptable conduct, integrity, or judgment on the part of the individual.”); *see also* DoDI 1320.04, Enclosure 4 at 1a (reciting the same).

⁸ The AAIP User Guide specifically states that the adverse summary in the AAIP database should not surprise the officer when it is served upon the officer prior to a promotion or HQDA selection board. *See* AAIP USER GUIDE *supra* note 4, at 11. However, it seems clear that an AAIP entry *could* surprise an officer. First, officers are not entitled to receive copies of approved AR 15-6 investigative findings on the Department of the Army (DA) Form 1574-1. Second, the AAIP User Guide explicitly states that officers do not have independent rights to view the summaries of credible adverse information, which are uploaded into the AAIP portal. AAIP USER GUIDE *supra* note 4, at 4. Third, the emphasis (both in training products and the user guide) on the fact that the synopsis and substantiated findings on the “summary of credible adverse information” must match the approved IO findings on the DA 1574-1, suggests that occasionally these items do not match. Given all of this, it seems obvious how the contents of an uploaded “summary of credible adverse information” in the AAIP database might surprise an officer when that summary is presented to them years later—especially where the underlying “adverse” conduct was minor and did not result in a reprimand or other adverse action.

⁹ Human Resources Command makes Soldier’s upcoming board files available for review and certification through a tool called the My Board File. *OSB or eSERB coming up? Better check ‘My Board File,’ Sgt. Michael Reinsch, 11 February 2014*, available at http://www.army.mil/article/119924/osb_or_eserb_coming_up_better_check_my_board_file. Consideration of AAIP entries is not limited to PSBs. Entries are also accessed for other Department of the Army (DA) selection boards. *See* AAIP USER GUIDE *supra* note 4, at 4.

half a decade has passed since the investigation. The witnesses are geographically dispersed throughout the world and some are no longer in the military. He does not have access to the high-priced counsel he hired years earlier. He lacks resources that were at his fingertips six years ago—resources that could assist him in responding to what he views as a significant inaccuracy in the database summary, which is to be presented to his PSB in a matter of weeks.

Captain Smith is fictional, but this general predicament is not.¹⁰ Neither AR 15-6 nor the AAIP User Guide impose upload notification requirements upon approval authorities (typically, but not always, commanders) or associated OSJAs responsible for uploading adverse findings into the AAIP database.¹¹ So, how could CPT Smith have accessed his AAIP summary prior to his My Board File opening for his O-4 PSB? The answer is in the Privacy Act of 1974.¹²

¹⁰ This observation is made based on the author's professional experience advising on Commanding General (CG) appointed investigations in two division-level administrative law shops as well as professional experience instructing on AAIP as an Associate Professor in Administrative and Civil Law at The Judge Advocate General's School. [Hereinafter Professional Experience]. This concern was raised by commanders in every Senior Officer Legal Orientation (SOLO) course the author instructed. If CPT Smith were a Reservist, he may not learn of his AAIP upload for nearly two decades until he reaches his O-6 board. *See* DoDI 1320.04 *supra* note 4 (noting that senate confirmation is not required for Reservist nominations until the rank of O-6). The AAIP database is not the only source of adverse information presented to PSBs. For Army promotion boards, adverse information is also pulled from the Army Law Enforcement Reporting and Tracking System (ALERTS), the Soldier's Army Military Human Resource Records (AMHRR), and the Inspector General Action Request System (IGARS). *See* Professional Experience. A surprising HRC adverse information notification could come from any of these systems of record. The AAIP database is not the sole source of interest when it comes to curiosity about what could exist in an agency system of records.

¹¹ *See* AR 15-6 *supra* note 2 at para. 2-1b (noting that special, personal, or principal staff officers or supervisors in the grade of major or above also have the authority to appoint, and therefore approve, preliminary inquiries or administrative investigations); *see also* AAIP USER GUIDE *supra* n. 4, at 10 (highlighting that if the approval authority is not a commander, the approval authority—not the commanders responsible for reviewing and approving the AAIP entry).

¹² The Privacy Act of 1974, as amended, 5 U.S.C. § 552a [hereinafter Privacy Act]; AAIP USER GUIDE *supra* n. 4 at 11.

In the spirit of enhancing trust and transparency in the Army Judge Advocate General's Corps (JAGC), this article aims to provide guidance on how individuals may use the provisions of the Privacy Act of 1974 and Army Regulation 25-22, *The Army Privacy and Civil Liberties Program* to request access to summaries of credible adverse information uploaded into the AAIP database.¹³ Section II of this article provides a brief overview of the development and current status of the AAIP. Section III explains the purpose and protections of the Privacy Act. Section IV outlines how officers can request access to AAIP entries. Finally, Section V argues that approval authorities should provide copies of credible adverse information uploaded into the AAIP database, which is the portal where this summary is stored) until the officer's applicable PSB or other Headquarters Department of the Army (HQDA) selection board.¹⁴ A template Privacy Act request form is included at the end of this article, which can be used to petition access to an entry in the AAIP database—a database that existed well before the program's expansion in February of 2023 through the publication of Army Directive (AD) 2023-03.

II. Army Directive 2023-03 and the Army's Adverse Information Program

In 2016, an update to AR 15-6 imposed requirements on approval authorities to upload AR 15-6 investigations with approved "adverse" findings into what is now known as the AAIP database.¹⁵ This upload requirement only applied to field-grade-officer subjects and

¹³ U.S. DEP'T OF ARMY, REG. 25-22, THE ARMY PRIVACY AND CIVIL LIBERTIES PROGRAM (30 Sep. 2022) [hereinafter AR 25-22]; AAIP USER GUIDE *supra* n. 4 at 4 (providing an example of what a summary of credible adverse information looks like).

¹⁴ This articles uses the words "portal" and "database" interchangeably to reference the electronic system of records where AAIP entries are stored.

¹⁵ AR 15-6 *supra* note 2, at para. 5-4e ("The right to respond to adverse information is extended by this regulation only to field grade officers, because such findings or recommendations may be considered in future promotion boards that will consider those officers for promotion.").

was required regardless of whether the investigation resulted in any adverse action against the field-grade-officer subject.¹⁶ In other words, even if the approval authority did not believe a reprimand or punitive action was appropriate to address the substantiated behavior—federal law nonetheless required the approval authority to upload the substantiated finding into the AAIP database. The database’s original purpose was to provide the Senate with additional information to use in determining whether an officer, with potential for General Officer (GO) promotion, met exemplary conduct requirements.¹⁷ As such, initially, the AAIP portal would only be accessed for officers considered before GO PSBs.¹⁸ For most officers, the entry would sit—un-accessed—for the remainder of the officer’s career. However, in the Fiscal

¹⁶ *Id.* at para. 3-19b(1) (“In the case of an investigation . . . that contains adverse information regarding a field-grade officer, the approval authority will keep the original and digital copy of the final report of proceedings, and the redacted version provided to the officer. This is done in accordance with para. 2-8c, on file for a period of not less than 10 years, regardless of whether any adverse action was taken against the officer based on the findings and/or recommendations of the investigation . . .”). If an approval authority determines that a finding is “adverse,” per the broad definition, outlined *supra* in note 7, upload is mandatory even where the commander takes no corrective action in response to the underlying adverse behavior. Given this requirement, the substantiated finding itself will leave a semi-permanent “adverse” mark in the officer’s record even if the commander purposefully chooses not to issue a permanently-filed reprimand. The mark is “semi-permanent” because, unlike a General Officer Memorandum of Reprimand which will be considered at every promotion selection board (PSB) the officer ever has, an adverse AAIP entry could be removed after 10 years and will not be considered (again) by the Senate unless and until the officer comes before a General Officer (GO) Promotion Selection Board (PSB). *See* DoDI 1320.04 *supra* n. 4, at encl. 4 (detailing the 10-year rule and previous-senate-consideration exclusion).

¹⁷ *See* 10 U.S.C. § 615(a)(3)(A) (“In the case of an eligible officer considered for promotion to a grade [requiring Senate confirmation] any credible information of an adverse nature, including any substantiated adverse finding or conclusion from an officially documented investigation or inquiry, shall be furnished to the selection board in accordance with standards and procedures set out in the regulations prescribed by the Secretary of Defense”); *see also* 10 U.S.C. § 7233 (“All commanding officers and others in authority in the Army are required—(1) to show themselves is good example of virtue, honor, patriotism, and subordination; (2) to be vigilant in inspecting the conduct of all persons who are placed under their command; (3) to guard against and suppress all dissolute and immoral practices, and to correct, according to the laws and regulations of the Army, all persons who are guilty of them; and (4) to take all necessary and proper measures, under the laws, regulations, and customs of the Army, to promote and safeguard the morale, the physical well-being, and general welfare of the officers and enlisted persons under their command or charge.”).

¹⁸ *See id.*; *see also* DoDI 1320.04, encl. 3 (“The Secretaries of the Military Departments will [e]nsure officers whose names are forwarded continue to remain qualified for promotion or appointment and meet the exemplary conduct provisions.”).

Year 2020 National Defense Authorization Act (NDAA), Congress required this PSB adverse screening process (previously only applicable to officers being considered for GO promotion) to apply to *all* officer promotions requiring United States Senate confirmation (O-4 and above on Active-Duty and O-6 and above in the Reserves).¹⁹ Thereafter, the Fiscal Year 2021 NDAA mandated that Special Selection Review Boards (SSRB) be held for any officer considered for promotion “to a grade at or below the grade of major general” if the officer’s file contained “credible information of an adverse nature,” which was not furnished directly to the promotion board itself.²⁰ To give these congressional changes effect, on 22 February 2023, the Secretary of the Army (SECARMY) published AD 2023-03.²¹

As of 24 March 2023, AD 2023-03 requires approval authorities to upload, into the AAIP portal, approved adverse findings from AR 15-6 investigations against *all* commissioned officers.²² The approval authority, with the assistance of the OSJA, must draft a “summary” of the approved adverse findings for upload into the AAIP database.²³ This entry is entitled the “summary of credible adverse information.”²⁴ A version of the summary of the approved

¹⁹ National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, § 502 (2019) [hereinafter FY20 NDAA]. Prior to this statutory change, adverse information was only required to be provided to Army promotion boards considering officers to promotion to “a grade above colonel.” *Id.*

²⁰ National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 628 (2020) [hereinafter FY21 NDAA]. Prior to AD 2023-03, the Army’s systems only tracked adverse findings for field grade officers, so it was not possible for the service to hold the required SSRB for a company grade officer whose credible adverse findings had never been uploaded.

²¹ AD 2023-03 *supra* n. 3. As mentioned, this directive expanded upload and due process requirements from field grade officers to all commissioned officers.

²² *Id.*

²³ *Id.*

²⁴ AAIP USER GUIDE *supra* n. 4 at 3.

adverse finding(s) is provided directly to the PSB charged with considering the officer-subject for their next Senate-confirmed promotion.²⁵

The AAIP User Guide states that the AAIP summary is “generally one page” in length.²⁶ The following information must be included in this one-page “summary”: (1) the officer’s name, (2) the approval authority’s name, (3) the source of information, (4) approval date, (5) “verbatim” approved findings,²⁷ (6) a written “synopsis” that “matches” the Department of the Army (DA) Form 1574-1 (Report of Proceedings by Investigating Officer),²⁸ (7) disposition and action taken in response to the finding (as documented on DA 1574-1), (8) the commander’s name, and (9) an optional commander’s comment, which is meant to

²⁵ See *supra* note 5; AAIP USER GUIDE *supra* n. 4 at 3 (“The ‘adverse summary’ is the Portable Document Format (PDF) document created by the AAIP system reflecting the date entered by the servicing legal office. By authorizing the adverse summary, the approving authority is directing the official submission of the adverse information into AAIP . . . The AAIP system produces a ‘Summary of Credible Adverse Information’ (the adverse summary referenced above) for each approved finding in the system. This adverse summary, generally one page, is what would be presented at a future PSB.”).

²⁶ AAIP USER GUIDE *supra* n. 4 at 3.

²⁷ See *id.* at 3-4. The “legal office” is responsible for entry and anyone within that legal office can draft findings and synopsis required to be uploaded into the system. Many offices use paralegals to draft these entries. See Professional Experience *supra* n. 10. The example summary and synopsis on page 4 of the AAIP user guide provides an excellent example of how concise this, “generally one-page” summary can be. *Id.* To this point, there could be confusion in the field about what exactly goes in the “approved findings” block and what goes in the “synopsis” block. *Id.* The updated user guide states that substantiated findings should be entered “verbatim.” AAIP USER GUIDE *supra* n. 4 at 3 (emphasis added). The requirement for a verbatim inclusion of approved findings can confuse legal offices when the guide states that information included in the “synopsis” block also “*must match* the information contained in the approved DA 1574-1 and/or Investigating Officer’s Findings and Recommendations Memorandum.” *Id.* at 7 (emphasis added). This is somewhat confusing and suggests that the exact information from the DA 1574-1 should be replicated in each of these blocks. It can also prove difficult (particularly in complex investigations with lengthy and detailed findings or in investigations where IOs were inartful, not concise, or poor writers) to put verbatim data in these blocks. See Professional Experience *supra* n. 10. Further, there are many legal offices that are not aware of this “verbatim” requirement at all and instead summarize approved findings and synopsis themselves to make these entries more concise and digestible. *Id.*

²⁸ The set-up of the portal is somewhat confusing. The portal itself suggests that the “synopsis” should be longer than the approved findings. The block for approved findings is smaller than the synopsis block, despite the fact that there is no character limit. The approved findings are also meant to be entered “verbatim” but, again, a “verbatim” entry does not appear to be required in the synopsis block. See AAIP USER GUIDE *supra* n. 4 at 3-4; see also *supra* n. 26.

provide the PSB or HQDA board with additional information and perspective on the underlying investigation or its findings.²⁹ Entries in the AAIP database are retrievable by the officer-subject's PII, including name, Department of Defense identification number (DODID), and social security number (SSN).³⁰ Entries include the subject's email address, rank, and unit identification code (UIC).³¹ The user guide also requires upload of investigatory materials, including the DA 1574-1, the IO's findings and recommendations memorandum, proof of service indicating the proposed adverse findings were provided to the subject, the written legal review, the complete un-redacted investigation, the subject's rebuttal matters, and a written determination the approving authority found the investigation to contain "adverse" information.³²

Given the necessity of this information (combined with the fact that IOs are not always concise and conclusory when drafting findings), legal offices tend to exercise discretion when drafting "summary" reports.³³ This includes summarizing, re-wording, or condensing lengthy or complicated adverse findings for the "summary of credible adverse information" page uploaded into the database.³⁴ Unfortunately, failure to use the exact language approved on the DA 1574-1 can contribute to confusion and surprise when the officer-subject sees the summation weeks, months, or years later.³⁵ Although, the initial referral and rebuttal process

²⁹ AAIP USER GUIDE *supra* n. 4 at 4.

³⁰ *Id.* at 6.

³¹ *Id.*

³² *Id.* at 7-8; *see supra* n. 7 (providing the definition of adverse).

³³ *See* Personal Experience *supra* n. 10.

³⁴ *Id.*

³⁵ *See supra* n. 8 (explaining how an officer-subject could be surprised by an HRC notification of an AAIP upload that they never knew existed).

put officers on notice that potentially approved adverse findings will be provided to future PSBs,³⁶ the officer subject will, in most cases, never know: (1) what version of the findings the approval authority approved after he reviewed the respondent's rebuttal matters; (2) whether the approval authority decided the finding was "adverse" and directed AAIP upload; or (3) how (or if) the approved adverse findings documented on the DA 1574-1 were reworded or "summarized" on the summary of credible adverse information uploaded into the database.³⁷

Approval authorities have the power to approve, disapprove, modify, or otherwise adjust an IO's recommended findings.³⁸ It is entirely possible an approval authority will modify an IO's findings after reading the subject's rebuttal matters.³⁹ Any substituted and approved finding is what the legal office would ultimately upload and, potentially, condense for the one-page portal summary.⁴⁰ This typically takes place without the subject-officer's knowledge.

³⁶ Because an AAIP upload has the potential to destroy an officer's promotion potential, AR 15-6 adds additional safeguards where adverse findings are concerned. The most important of these safeguards is the referral of the report and opportunity for rebuttal. AR 15-6 *supra* n. 2 at para. 5-4. The referral of adverse information is disparate in the field. *See* Professional Experience at n. 10. Paragraph 5-4 states that the officer should receive, "the portion of the report of investigation and supporting evidence pertaining to the adverse information." AR 15-6 at para. 5-4. Some offices provide officers with the full investigation with minimal redactions. Other offices provide heavily-redacted portions of the findings memorandum and only some pieces of heavily-redacted evidence that the legal office has determined are pertinent to the adverse finding. Varying interpretations of this paragraph can create disparity in the field when it comes to an officer's ability to submit a meaningful rebuttal capable of influencing an approving authority not to upload into AAIP. *See* Professional Experience *supra* n. 10.

³⁷ AAIP USER GUIDE *supra* note 4 at 3; *see also supra* n. 8.

³⁸ AR 15-6 *supra* n. 2, at para. 2-8b. This is provided that the modified findings are supported by the preponderance of the evidence as ensured by the written legal review. *Id.*

³⁹ *See id.* (noting that such a change is appropriate provided that the adjusted finding is consistent with the evidence included in the report of proceedings).

⁴⁰ AAIP USER GUIDE *supra* note 4 at 7 ("The entry must reflect, verbatim, the finding as it appears in the approved investigation as modified or substituted, if applicable, by the investigation's approval authority."). In

The current process requires some officers to wait up to two decades to see a version of the summary the OSJA uploaded into the AAIP portal.⁴¹ Even though there is *no prohibition* on releasing this adverse summary,⁴² in the vast majority of cases, it is not until the officer receives an HRC notification alerting them to the existence of adverse information in their board file that the officer can access and inspect a version of the summary of credible adverse information the legal office drafted and filed in the AAIP database.⁴³ Even if an OSJA provides notification that the approval authority uploaded an AAIP entry, it is exceedingly rare for an OSJA to share the exact language documented on the “summary of credible adverse information” uploaded into the portal—even where that language could play a non-minor role in a future promotion board for the officer-subject.⁴⁴

In cases where officer investigations or AAIP upload are not withheld to the Commanding General (CG), it is common for the brigade legal shop to enter the synopsis and

this author’s opinion, a second referral should be executed if the findings were amended in a way that was adverse to the subject. Much like the AAIP entry, officers are not entitled to the approved investigatory findings on the finalized DA 1574-1.

⁴¹ Army Directive 2023-03 requires that adverse findings against company grade officers in the Reserve Component be entered into the AAIP portal. AD 2023-03 *supra* n. 3. However, the first Reserve Component promotion is the O-6 PSB. *See* DoDI 1020.03, encl 6 *supra* n. 4. As such, a company-grade Reservist, whose commander uploaded an adverse finding against them into the portal may not see a version of that entry for twenty years.

⁴² AAIP USER GUIDE *supra* note 4 at 11.

⁴³ *Id.* (“The notice and opportunity to respond process for AAIP adverse summaries only occurs when, and if, a finalized summary of credible adverse information is produced pursuant to an officer’s consideration by a DA selection board where adverse information concerning the officer will be considered.”) Again, the “summary of credible adverse information,” provided to a promotion selection board, captures all adverse information from the systems of record mentioned above in footnote 10 (AAIP, AMHRR, ALERTS, and IGARS). As such, the summary drafted by the OSJA may not be the same summary presented to the board. *See* AAIP USER GUIDE at 3. It seems possible that the OSJA’s summary could be even further summarized when all credible, adverse information is compiled at the time of the board.

⁴⁴ *See supra* n. 36; *see also* Professional Experience.

summary into the AAIP portal.⁴⁵ Many offices use paralegals, who may not understand the significance of the entry, to draft and upload the synopsis and summary.⁴⁶ Additionally, and significantly, the updated AAIP User Guide removed the requirement that the installation SJA or DSJA personally review every AAIP entry prior to finalization.⁴⁷ This could mean the highest-level legal review an AAIP entry gets is by a new Chief of Administrative Law or Command Judge Advocate with minimal to no experience dealing with AAIP.⁴⁸ This is important given that the AAIP entry will be used in a manner similar to a General Officer Memorandum of Reprimand (GOMOR), which presumably would receive a legal review from a seasoned field-grade attorney prior to a General Officer directing placement in an officer's official military personnel file (OMPF).⁴⁹

Based on the foregoing—to include removal of an elevated legal review by the installation SJA—it remains entirely possible that the summary in the AAIP database does

⁴⁵ AAIP USER GUIDE *supra* n. 4, at 7, 10. The previous user guide required that all AAIP entries be reviewed by either the SJA or DSJA. ADVERSE INFORMATION PILOT PROGRAM (AIPP) USERS' GUIDE V. 1.0 (September 2016) at 2. Updated guidance now requires the approval authority's "legal advisor" review the entry. AAIP USER GUIDE *supra* n. 4, at 3. Depending on withholding policies and organizational structures, this normally means the Chief of Administrative Law's review (with no rank or experience requirement attached) has replaced the mandatory installation SJA or DSJA review. Again, this AAIP entry will play some role in forthcoming HQDA and/or promotion selection boards with limited and untimely recourse available to the impacted officer. *See id.* at 9 (outlining that once an AAIP entry is approved it can only be modified to correct an "administrative error in the entry" or upon a change to the underlying findings).

⁴⁶ *See* Personal Experience *supra* n. 10. This assertion is based on instruction provided to paralegals on AAIP and administrative investigations from 2021-2023. Generally, the student audience was unaware of the significance of AAIP entries, which many in the audience reported personally drafting with minimal oversight through their own access of the AAIP portal. Today, with increased emphasis and education on AAIP, this is hopefully changing.

⁴⁷ AAIP USER GUIDE *supra* n. 4 at 3. Even when the SJA or DSJA review was mandated by the user guide, it was common in the field for this review not to occur. *See* Personal Experience *supra* n. 10.

⁴⁸ *Id.* at 13 (outlining that prior to entry it is sufficient that the Chief of Administrative Law or a civilian legal advisor review the entry).

⁴⁹ An AAIP entry is not a "permanent" filing and is not the same as a General Officer Memorandum of Reprimand (GOMOR), which remains in the recipient's official military personnel file throughout the duration of their career. *See supra* n. 16 (explaining how AAIP entries differ from GOMORs).

not match the approved finding and is inconsistent with a verbatim recitation of the IO's findings memorandum attached to the DA 1574-1. Again, this is significant given that the summary will later be used to determine the officer's upward career progression.⁵⁰ Despite all of this, current Army practice is, generally, *not to provide* AAIP filing notification and contents to officer-subjects.⁵¹ As such, officers should understand how to utilize Privacy Act protections to request access to AAIP entries.

III. The Privacy Act

A. History of the Privacy Act

Many think of the Privacy Act as a tool to protect their personal information. While this is true, the Privacy Act does more than merely prevent the dissemination of PII. It also facilitates trust between federal agencies and the American people by mandating transparency.⁵² The Act requires federal agencies to comply with specific processes and procedures for collecting, maintaining, using, and disclosing information about individuals when said information is maintained in a system of records.⁵³

The Privacy Act was enacted following the Executive Branch's abuse of the American people's trust.⁵⁴ Immediately before the enactment of the Privacy Act, the

⁵⁰ A scrub of the entry and associated investigation does occur prior to the promotion or HQDA selection board at the Office of The Judge Advocate General Administrative and Civil Law Division level. This scrub is meant to ensure that the summary matches the approved finding.

⁵¹ This assertion is based off the understanding that it is considered "best practice" not to provide AAIP upload contents to the respondent. It is also based off the emphasis on the lack of an independent right to access detailed in the user guide. AAIP USER GUIDE *supra* n. 4, at 4.

⁵² See S. Comm. on Gov't. Operations & H.R. Comm. on Gov't. Operations, 94th Cong., Legislative History of the Privacy Act of 1974 S. 3418 (Public Law 93-579)

⁵³ *Id.*; U.S. Department of Justice (DOJ), Overview of the Privacy Act of 1974, 2020, <https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition>.

⁵⁴ Congressional Research Services. (Dec. 27, 2023). *The Privacy Act of 1974: Overview and Issues for Congress*. (CRS Report No. R47863). <https://crsreports.congress.gov/product/pdf/R47863>.

executive branch, under President Richard Nixon, was involved in the illegal surveillance and collection of personal information on U.S. citizens.⁵⁵ News outlets “exposed a massive CIA domestic spying operation against protesters, civil rights activists, and other dissenters, which set the stage for the creation of The Privacy Act of 1974.”⁵⁶ The bill’s principal sponsor, Judiciary Chairman Senator Sam Ervin, stated that “[i]f we have learned anything in this last year of Watergate, it is that there must be limits upon what the Government can know about each of its citizens.”⁵⁷ Thereafter, President Nixon resigned the presidency and President Gerald Ford signed the Privacy Act into law in January 1975.⁵⁸

Ultimately, the Executive’s covert collection of information on individuals—combined with the increased capability of technology to electronically collect and store large amounts of data—contributed to a growing distrust of the government and increased public concerns about government transparency.⁵⁹ The Privacy Act was intended to “restore trust in government and to address what at the time was seen as an existential threat to American democracy.”⁶⁰ Practitioners should consider this historical context when analyzing the Privacy Act’s implications in the AAIP process.

⁵⁵ <https://www.washingtonpost.com/wp-srv/national/longterm/watergate/articles/061872-1.html>.

⁵⁶ Widener Law Review 2013, *The Invasion of Privacy Act*, at 350.

⁵⁷ See S. Comm. on Gov’t. Operations & H.R. Comm. on Gov’t. Operations, 94th Cong., *Legislative History of the Privacy Act of 1974* S. 3418 (Public Law 93-579).

⁵⁸ <https://www.usatoday.com/story/news/2022/08/09/when-did-richard-nixon-resign/10275787002/>.

⁵⁹ Secretary’s Advisory Committee on Automated Personal Data Systems. (1973). *Records, Computers, and the Rights of Citizens: Report* (Vol. 10). U.S. Department of Health, Education & Welfare.

⁶⁰ U.S. Department of Justice (DOJ), *Overview of the Privacy Act of 1974, 2020*, <https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition>.

B. Army System of Record Notification

The Privacy Act aims to balance the government's need to collect and maintain information on individuals with individual privacy rights.⁶¹ The Privacy Act accomplishes this by requiring agencies to publish detailed notifications to the public when an agency collects and stores PII.⁶² Specifically, the Privacy Act mandates that agencies publish a System of Records Notification (SORN) in the Federal Register upon establishing—or significantly modifying—a System of Records (SOR) that the agency maintains.⁶³

At the service level, AR 25-22 requires Army activities to publish notices of all Army SORs in the Federal Register when a new SOR is established or (important here to this AAIP discussion) when significant changes are made to an existing SOR.⁶⁴ Per regulation, significant changes are those “that are substantive in nature and therefore warrant a revision of the SORN to provide notice to the public of the modified SOR.”⁶⁵ Significant changes include (1) modifications to the number or type of individuals on whom records are kept, (2) the expansion of the types or categories of information maintained, and (3) changes to the purpose for which the information is used.⁶⁶ AR 25-22, para. 3-1.

⁶¹ See S. Comm. on Gov't. Operations & H.R. Comm. on Gov't. Operations, 94th Cong., Legislative History of the Privacy Act of 1974 S. 3418 (Public Law 93-579).

⁶² See generally 5 U.S.C. § 552a.

⁶³ 5 USC § 552a(a)(3); 5 U.S.C. § 552a(e)(4).

⁶⁴ See AR 25-22 para. 3-1 *supra* n. 13.

⁶⁵ *Id.*

⁶⁶ *Id.*

Consistent with the Privacy Act, Army regulation lists what information must be included in public notification, which is accomplished through publication in the Federal Register.⁶⁷ The SORN must contain the following: (1) name and location of the system; (2) categories of individuals on whom records are maintained; (3) categories of records maintained in the system; (4) each routine use of the records contained in the system, including the categories of users and the purpose of such use; (5) policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records; (6) title and business address of the agency official who is responsible for the system of records; (7) agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him; (8) agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content; (9) and categories of sources of records in the system.⁶⁸ These details inform the public (to include impacted individuals) what information the agency collects and maintains. However, for the Privacy Act to apply, the information must first meet the definition of a “record” and be part of a “system of records.”⁶⁹

C. Army System of Records

A record is “any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education . . . criminal or employment history and that contains his name, or the identifying number, symbol, or other

⁶⁷ *Id.*

⁶⁸ 5 U.S.C. § 552a(e)(4).

⁶⁹ *Id.*

identifying particular assigned to the individual, such as a finger or voice print or a photograph.”⁷⁰ For example, officer evaluation and combat fitness reports are records under the Privacy Act.⁷¹ They are physical documents that the Army maintains, which include identifying particulars like the individual’s name. Once the information is identified as a record, the next requirement is to determine whether the record is part of a system of records.

Privacy Act litigation against the government often focuses on this “system of records” concept.⁷² A system of records is a “group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.”⁷³ Army Regulation 25-22 defines a system of records similarly, but clarifies that a system of records can be digital or physical.⁷⁴ For example, finalized military justice investigations, trials by courts-martial, and other administrative or disciplinary proceedings stored in Military Justice Online (MJO)—or even an OSJA file cabinet—may be considered a SOR.⁷⁵ Such records are typically indexed by an individual’s name and retrievable by the individual’s PII. The inclusion of clarifying language in AR 25-22 regarding electronic or

⁷⁰ *Id.*

⁷¹ *See id.* (providing the definition of a record).

⁷² *See e.g.*, *Maydak v. United States*, 363 F.3d 512, 519-20 (D.C. Cir. 2004) (remanding case to district court to determine whether prisons’ compilation of photographs constitutes system of records); *Burton v. Wolf*, 803 F. App’x 120, 122 (9th Cir. 2020) (concluding that records were not in a system of records under the Privacy Act because they were “retrievable only with the identifying information of his estranged wife in her A-File, not his own”); *Kearns v. FAA*, 312 F. Supp. 3d 97, 108 (D.D.C. 2018) (concluding that requested documents were not retrieved from system of records because they were not retrieved by plaintiff’s name or identifier but by the case number).

⁷³ 5 U.S. Code § 552a(a)(5).

⁷⁴ AR 25-22 para. 3-1 (defining a SOR as “a group of records, whatever the storage media (paper or electronic), under the control of an Army activity . . .”).

⁷⁵ Military Justice Online is an Army JAG Corps tool for creating, storing, and tracking military justice-related documents and information.

paper storage is consistent with concerns that led to the enactment of the Privacy Act. The AAIP database, and the information stored therein, is an example of precisely the type of product and capabilities the drafters of the Privacy Act intended to regulate.⁷⁶

It is clear that AAIP entries constitute “records” per the term's statutory definition.⁷⁷ The AAIP database is maintained by the Army, contains personal and adverse information about the officer, and is retrievable by the officer’s PII in the form of name, DODID, unit of assignment, and similar data. Those with access to the database can retrieve the record using the officer-subject’s SSN or other identifying information. Whether the AAIP database, standing alone, is a “system of records” is more complicated.

The SORN that captures the information contained and uploaded into the AAIP database is the “General Legal Files” SORN, which covers legal investigations.⁷⁸ This SORN was published in the Federal Register on December 8, 2000—fifteen years before the Army’s Adverse Information Pilot Program was established and sixteen years before AR 15-6 received its most recent update.⁷⁹ As mentioned, AR 25-22 requires the publication of significant changes to existing SORs.⁸⁰ Given (1) the creation of the AAIP database in 2015, (2) the program’s significant expansion mandated by the FY20 NDAA, (3) the Army’s expansion of the AAIP program in 2023, and (4) associated changes regarding how the Army

⁷⁶ See S. Comm. on Gov’t. Operations & H.R. Comm. on Gov’t. Operations, 94th Cong., Legislative History of the Privacy Act of 1974 S. 3418 (Public Law 93-579).

⁷⁷ 5 U.S.C. § 552a(4) (providing the statutory definition of record).

⁷⁸ 65 Fed. Reg. 77002 (8 Dec 2000).

⁷⁹ *Id.*

⁸⁰ AR 25-22 para. 3-1.

now uses adverse findings from legal investigations, there is a strong argument that the Army should create a separate SORN for the AAIP database, or at least publish a modification of the existing SORN.⁸¹

It is also worth noting that the inclusion of a “commander’s comment” in the AAIP database is a significant change from information understood to be covered by a legal investigation in December 2000. The commander’s comment allows the commander to provide “additional context or perspective regarding the investigation’s findings.”⁸² The comment is consequential because DA selection and promotion boards see this comment and consider it when deciding whether to recommend the officer for promotion or selection.⁸³ This is, arguably, a significant departure from the information the SOR originally collected and maintained. Despite these significant changes, the current SORN has not been updated to reflect what is now collected and maintained by the SOR in accordance with AAIP upload requirements.

⁸¹ Pippinger v. Rubin, 129 F.3d 519 (1997). There is case law that supports the AAIP database, standing alone, is not a SOR. In Pippinger, the plaintiff, a federal employee, claimed the Privacy Act prohibited the Internal Revenue Service (IRS) from maintaining disciplinary records of its employees in the Automated Labor Employee Relations Tracking System" (ALERTS), because the name and location of the system was never published in the Federal Register. The ALERTS system was a summary of information contained in two authorized SORN that were published in the Federal Register. In ruling the ALERTS system was not a SOR, the 10th circuit court held that the abstraction of records from a lawfully maintained system of records does not, standing alone, create a new system of records, so long as the abstraction is used for the purpose already published in the Federal Register and cannot be accessed by anyone not already identified in the notification. In Pippinger, the issue was whether the agency violated the Privacy Act by disclosing information contained in ALERTS and not establishing a new or modified SORN in the Federal Register specifically addressing ALERTS. It is the author’s belief the court would rule differently if the issue was whether ALERTS was a system of records for the purpose of determining whether an individual had the right to access their own information under the Privacy Act. This argument is largely beyond the scope of this article, but important with respect to whether the AAIP database and the program’s expansion mandate statutory changes.

⁸² AAIP USER GUIDE *supra* n. 4 at 12.

⁸³ *Id.*

In sum, the SOR covered by the “General Legal Files” SORN has been significantly modified in that: (1) the number of type of individuals on whom records are kept has changed given 2023 requirements to upload adverse findings for all commissioned officers, (2) that category of information maintained has changed in that we now include “commanders comments” in the database, and (3) the purpose for which the information is used has changed given that uploaded data is now provided directly to DA promotion and selection boards.⁸⁴ Given these critically important change to both the information stored and its use, the existing SORN should be modified or a new SORN should be created.

Regardless, it is indisputable that adverse entries placed in the AAIP portal are subject to the Privacy Act and may be lawfully accessed by the officer whose record was uploaded into the portal.

D. The Right of Access Under the Privacy Act

For drafters of the Privacy Act, “one of the most obvious threats the computer poses to privacy comes in its ability to collect, store, and disseminate information without any subjective concern for human emotion and fallibility.”⁸⁵ As a result, the legislation granted individuals the right to access certain records about themselves contained in a system of records.⁸⁶ This statutory right of access under the Privacy Act also permits individuals to request amendment of their records should they believe their records are not “accurate, relevant, timely, or complete.”⁸⁷ Individual requesters may also authorize a third party to

⁸⁴ See AR 25-22, para. 3-1 (explaining when a new SORN is required).

⁸⁵ INTRODUCTORY REMARKS OF SENATOR SAM J. ERVIN, JR., ON S. 3418.

⁸⁶ 5 U.S.C. §552a(d).

⁸⁷ 5 U.S.C. §552a(d)(2).

access their record, provided the authorization is in writing.⁸⁸ In response to a request to amend a record by an individual, federal agencies must inform the individual of whether it will make the requested correction, or, if the agency refuses, it must provide and explain to the individual the reason for the refusal and include the appropriate agency procedures to request a review of the agency’s decision.⁸⁹ Although the right to access information is not exclusive to the Privacy Act, it is the primary authoritative source for individuals requesting information about themselves. However, the right to access under the Privacy Act should not be confused with an individual’s statutory right to request records from federal agencies under the Freedom of Information Act (FOIA).⁹⁰

The Freedom of Information Act and the Privacy Act serve very different purposes. The “Privacy Act is designed to maintain trust between individuals and agencies in connection with the collection, use, and dissemination of records pertaining to them, the FOIA is designed to increase the public’s access to governmental information.”⁹¹ Additionally, the FOIA creates a statutory right for “any person” to request federal agency records.⁹² Under the FOIA, “any person” includes an “individual, partnership, corporation, association, or public or private organization other than an agency.”⁹³ In contrast, under the Privacy Act, the right

⁸⁸ 5 U.S.C. § 552a(b).

⁸⁹ 5 U.S.C. §552a(d)(1)-(2).

⁹⁰ 5 U.S. Code § 552. Although the Privacy Act is most applicable, litigants often cite causes of action under both the Freedom of Information Act (FOIA) and Privacy Act because the FOIA statute includes a fee shifting provision, permitting the trial court to award reasonable attorney fees and costs to prevailing plaintiffs. 5 U.S.C. 552(a)(4)(E)(i) (2018).

⁹¹ DOJ, Office of Information Policy, “OIP Guidance: The Interface Between the FOIA and Privacy Act,” September 30, 2022, <https://www.justice.gov/oip/oip-guidance-interface-between-foia-and-privacy-act>.

⁹² 5 U.S.C. § 552.

⁹³ 5 USC § 551(2).

to access records only applies to U.S. citizens and aliens lawfully admitted for permanent residence.⁹⁴

IV. How to Request an AAIP Entry

Army Regulation 25-22 is the Army's governing authority on access to individual records. The regulation grants both the right to access and the opportunity to amend records contained in an Army SOR.⁹⁵ All Army SORs are listed on the Army Records Management Division (ARMD) website.⁹⁶ Requests for access to records must be submitted to the program manager or the custodian of the record designated in the published SORN.⁹⁷ The SORN includes what must be contained in the request and to whom the request should be addressed.⁹⁸ Generally, the request should be in writing, and the requester's identity should be verified.⁹⁹ There is no requirement to state a reason or justify the need to gain access to records; however, requesters should reasonably describe the records they are requesting.¹⁰⁰ Once an individual requests access to their record, the Privacy Act requires agencies to acknowledge receipt not later than ten days (excluding Saturdays, Sundays, and legal public holidays).¹⁰¹ The custodian must forward requests for information recommended for denial to

⁹⁴ 5 U.S.C. § 552a(a)(2).

⁹⁵ AR 25-22 para. 6-1.

⁹⁶ <https://www.rmda.army.mil/privacy/sorns/armypublishedsorn.html>. Similarly, all Department of Defense (DoD) SORs are listed on the DoD Component Privacy Office website. <http://www.defense.gov/privacy>.

⁹⁷ AR 25-22 para. 6-2.

⁹⁸ *Id.* at para. 3-1.

⁹⁹ *Id.* at para. 6-2.

¹⁰⁰ *Id.* at para. 6-2(c).

¹⁰¹ 5 U.S.C. § 552a(d).

the appropriate denial authority, along with a copy of the request, disputed records, and justification for withholding the information.¹⁰² Additionally, Army Regulation 25-55 lists the appropriate denial authorities based on the requested record. If an access request is denied, within 30 working days, the Initial Denial Authority (IDA) must notify the requester and state the reasons for denial.¹⁰³ Army Regulation 25-22 lists the information that must be included in the denial notification, including notification to the Office of the General Counsel.¹⁰⁴

In accordance with the established SORN and AR 25-22, an individual requesting access to their own AAIP entry should address written inquiries to the Department of the Army, Office of the Judge Advocate General, 2200 Army Pentagon, Washington, DC 20310-2200.¹⁰⁵ The request must be in writing and should include the requester's full name, address, telephone number, and any other personal data which would assist in identifying the relevant records.¹⁰⁶

The requesting individual must also verify their identity.¹⁰⁷ A notarized signature is sufficient for verification.¹⁰⁸ Alternatively, a requester may verify their identity by providing

¹⁰² AR 25-22 para. 6-2.

¹⁰³ *Id.*

¹⁰⁴ The denial notification must include, among other things, the reason for denial and the right to administratively appeal the denial within 60 calendar days of the mailing date of the notice, through the denial authority, to the Office of the General Counsel, Secretary of the Army, at 104 Army Pentagon, Washington DC 20310-0104. AR 25-22 para. 6-6.

¹⁰⁵ <https://dpcl.d.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/569945/a0027-1-daja/>.

¹⁰⁶ AR 25-22 para. 6-2.

¹⁰⁷ *Id.*

¹⁰⁸ *Id.*

an unworn declaration per 28 USC § 1746.¹⁰⁹ In this case, the record's custodian, OTJAG, or the applicable OSJA (if the authority is delegated) will have 10 working days to acknowledge the request for access made under the Privacy Act.¹¹⁰ The custodian must then provide access to the requested records within a reasonable timeframe, generally within 30 days.¹¹¹

V. *In Sum: Due Process, Policy Change, and AAIP*

It is the opinion of these authors that approval authorities should—at the time of upload—voluntarily share summaries of credible adverse information with officers whose PII is uploaded into the AAIP database. Temporally, this is when the officer is in the best position to remediate inaccuracies, collect witness statements, utilize current resources, and make career decisions based on the facts and contents of the upload. However, this recommendation runs contrary to current policy. This is presumably because such notification can create challenges for approval authorities and associated OSJAs.

One argument against notifying officers of the AAIP filing is that no due process is associated with the filing decision (or the contents of the uploaded materials) at the time of upload; rather, the due process right instead exists at the time the adverse information is set to be presented to a PSB or HQDA selection board.¹¹² There may be a concern that releasing summaries of credible adverse information will generate complaints, requests for process where none exists, complications for OSJAs across the field, and headaches for The Office of

¹⁰⁹ *Id.*

¹¹⁰ *Id.*

¹¹¹ *Id.*

¹¹² AAIP USER GUIDE *supra* n. 4, at 4. The AAIP User Guide provides that “Once an AAIP entry is approved, it can only be modified or removed to correct an administrative error in the entry at the time the Data Entry Approving Authority determined the finding(s) was adverse and directed the AAIP entry or upon a change to the underlying finding following reconsideration in accordance with AR 15-6, paragraph 2-9.” *Id.* At 9.

the Judge Advocate General's Administrative and Civil Law office (OTJAG ADLAW), which is the custodian of the records and manager of the AAIP database. The fact that the uploaded AAIP summary is subject to additional changes right before the applicable promotion or selection board, also complicates matters.¹¹³ However, these concerns do not outweigh the arguments in favor of voluntarily providing officers with the uploaded summary of their adverse information.

At the outset, notification of the summary of credible adverse information does not create a due process right. Instead, the notification provides the officer-subject with pertinent information at the time the officer is best positioned to deal with this information.

Notification would grant the officer knowledge that could inform career decisions and would provide transparency and enhance trust in commanders, our Corps, and our institution.

Commanders in the Senior Officer Legal Orientation (SOLO) course at The Judge Advocate General's Legal Center and School have consistently expressed dismay over the perceived secret nature of AAIP uploads.¹¹⁴ During my tenure as an instructor at the school, more than a dozen commanders approached me after class to request guidance on accessing SORs to determine whether adverse information had been uploaded into a system of records without their notification or knowledge in cases where they had been investigated but no adverse action had followed.¹¹⁵

¹¹³ See *supra* nn. 10 & 43 (explaining that the AAIP entry is only one aspect of the summary of credible adverse information that could ultimately be presented to a board and describing how the AAIP entry is reviewed and potentially edited in advance of the applicable board).

¹¹⁴ Personal Experience *supra* n. 10.

¹¹⁵ *Id.*

This article does not suggest officers should be granted a *de facto* rebuttal of uploaded AAIP summaries.¹¹⁶ In fact, the Privacy Act explicitly limits what an officer can contest: accuracy, relevancy, timeliness, and completeness.¹¹⁷ As mentioned above, summaries are often (as the name would suggest is entirely appropriate) summarized. They are frequently drafted by junior personnel, and updated policy guidance has removed the requirement for mandatory installation SJA or DSJA review prior to entry.¹¹⁸ Reasonable minds may disagree on whether a particular summary accurately reflects the approving authority's findings if those findings were not verbatim recitations from the DA 1574-1. Additionally, the AAIP entry may contain an administrative error or inaccuracy, which is precisely what the Privacy Act was designed to minimize. Even if the opportunity to amend the AAIP entry is denied, at a minimum, approval authorities should grant requests for access to view the entry.¹¹⁹ Not only will the information allow the officer to leverage current resources, it could also inform career decisions.

Approval authorities and OSJAs can assist in establishing a culture of transparency and trust—principles at the core of the Privacy Act—by putting people first and providing

¹¹⁶ Army Regulation 15-6 provides officer-subjects, against whom adverse findings have been made up to three rebuttals. First, officers are permitted to rebut the IO's findings and submit matters to the approval authority. AR 15-6 *supra* n. 2 at para. 5-4. The officer next can rebut any potential adverse action that is imposed based on the underlying adverse information. Finally, the officer can rebut—in the form of a comment to the PSB—the adverse information provided to the promotion board in the summary of credible adverse information.

¹¹⁷ AR 25-22 para. 8-2.

¹¹⁸ AAIP USER GUIDE *supra* n. 4 at 3 (noting that the approving authority's legal advisor can complete the necessary "personal review"); *see also* Professional Experience.

¹¹⁹ This suggested process change is similar to the notification procedures outlined in AR 600-37 for reprimand filing determinations. Cite applicable paragraph of AR 600-37. Army Regulation 600-37 requires General Officers to notify respondents regarding whether the General Officer Memorandum of Reprimand (GOMOR) was uploaded into their local file or their Army military Human Resource Record (AMHRR) permanently. *Id.*

officers with information uploaded into the AAIP portal at the time the approval authority files such information in the database.¹²⁰ Transparency and trust should serve as a compass to guide actions in the absence of a clearly defined rule or when circumstances appear ambiguous. Officers should not be unnecessarily restricted from knowing information that could drastically impact their career progression and, ultimately, their lives. Instead, approval authorities should voluntarily provide this information to the officer at the time of upload. Denying officers the opportunity to review the exact language uploaded into the SOR at the time of entry can leave a service member in the unenviable position in which our hypothetical CPT Smith found himself: receiving an HRC prompt to respond to negative, stale, and possibly surprising information weeks before the Army provides this data to a PSB or an HQDA selection board. On occasions where transparency feels as if it is lacking, Soldiers should know how to access their records and exercise their rights under the Privacy Act.

¹²⁰ www.dvidshub.net/video/454962/colin-powell-leadership.

TEMPLATE PRIVACY ACT REQUEST FORM

[Your Name]
[Your Address]
[City, State, ZIP Code]
[Email Address]
[Phone Number]

[Date]

Department of the Army
Office of the Judge Advocate General
2200 Army Pentagon
Washington, DC 20310-2200

Subject: Privacy Act Request - Copy of Records in the Army Adverse Information Database Pertaining to (Complete Name)

I am writing to request a copy of all my records stored in the Army Adverse Information Program Database. This request is submitted under the provisions of the Privacy Act of 1974, 5 U.S.C. § 552a and Army Regulation 25-22 para. 6-1.

The Privacy Act guarantees me the right to access and review personal information maintained by federal agencies, including the U.S. Army that is stored in a system of record. Accordingly, I am requesting information about me. To facilitate the processing of my request, I have attached proof of my identity and my notarized signature/unsworn statement under 28 USC 1746. Also, below is my information to assist with locating the applicable records.

1. Full Name: [Your Full Name]
2. Date of Birth: [Your Date of Birth]
3. DoD ID Number:
4. Phone Number:
5. Home Address:

I kindly request that you provide a copy of any adverse information about me in the Army Adverse Information Program Database, including, but not limited to, the adverse information summary. The information may be sent to my email [email address] or to my physical location at [mailing address]. Additionally, please inform me

of any additional specific requirements or procedures I must follow to access these records.

Under the Privacy Act, you must respond to my request within 30 days of receipt. If it is determined that some or all requested records cannot be released, I ask you to provide a written explanation citing the specific exemptions or legal basis for withholding such information. I am also aware that reasonable fees may be associated with processing my request, as allowed under the Privacy Act. If fees are applicable, please estimate the total cost of accessing and copying the requested records.

I appreciate your attention to this matter and your cooperation in fulfilling my request. If you have any questions or require additional information, please do not hesitate to contact me using the provided contact details. Thank you for your prompt attention to this request.

Sincerely,

[Your Name]