DEFENSE LEGAL SERVICES AGENCY
DEFENSE OFFICE OF HEARINGS AND APPEALS
APPEAL BOARD

Date: July 29, 2026

In the matter of:	)	
----------	)	ISCR Case No. 22-02555
Applicant for Security Clearance	)	

APPEAL BOARD DECISION

APPEARANCES

FOR GOVERNMENT
Andrea M. Corrales, Esq., Deputy Chief Department Counsel

FOR APPLICANT
Pro se

The Department of Defense (DoD) declined to grant Applicant a security clearance. On March 28, 2023, DoD issued a Statement of Reasons (SOR) advising Applicant of the basis of that decision – security concerns raised under Guideline K (Handling Protected Information) of the National Security Adjudicative Guidelines (AG) in Appendix A of Security Executive Agent Directive 4 (effective June 8, 2017) and DoD Directive 5220.6 (Jan. 2, 1992, as amended) (Directive). On May 26, 2026, Defense Office of Hearings and Appeals Administrative Judge Eric C. Price denied Applicant national security eligibility. Applicant appealed pursuant to Directive ¶¶ E3.1.28 and E3.1.30.

The SOR alleged 12 security concerns, primarily related to Applicant's duties as media custodian in a Special Access Program (SAP) facility (SAPF) during 2020 and 2021. Applicant admitted two allegations, denied the rest, and provided explanations. At hearing, the Government called four witnesses (GW1-GW4), and Applicant called five (AW1-AW5). The Judge found favorably for Applicant on six allegations and adversely on the remaining six. The Government did not appeal the favorable findings, and they are not in issue on appeal. The facts and circumstances surrounding those allegations will not be discussed other than in the context of the allegations that remain at issue.

Background

Applicant is in his early 40s and a cybersecurity specialist, with a bachelor's degree in management information systems, a master's degree in cybersecurity, and multiple certifications in the field, including Certified Information System Security Professional. Since 2008, he has worked for various defense contractors in information system administration and security positions, including as system and network administrator, communications security officer, and cybersecurity analyst. He has held a security clearance since 2008. His SAP access was suspended in August 2021 in the wake of the incidents alleged in the SOR.

In September 2019, Applicant was assigned as a contractor employee in a Service-level program management office (PMO or the "Organization"). At the time, the PMO had no in-house cybersecurity team, and Applicant was brought in to support its information systems capabilities and cybersecurity requirements. His primary duties were as the Organization Information System Security Manager (ISSM) and included responsibility for compliance with SAP regulations, as the PMO was standing up a SAPF.

In about March 2020, Applicant was also appointed as the media custodian for several information systems in the SAPF. His duties as media custodian included establishing control of all media (*e.g.*, CDs or DVDs) upon its entry into the SAPF and maintaining accountability for all media until destruction in accordance with controlling regulations. All but one of the SOR allegations arise from Applicant's duties as media custodian from his appointment in March 2020 until he was relieved of his duties in February or March 2021.

Applicant's media custodian duties required frequent interaction with security personnel, including the program security officer (PSO), a position with broad responsibility for the security of the SAPF (*e.g.*, enforcement of policies, approval of access, management of SAPF physical security, and oversight of classified document control). Applicant and witnesses described the working environment at the PMO, including within the SAPF, as fast-paced and strained by professional and personal conflicts between the cybersecurity team and security personnel. In December 2020, a new PSO (the Organization PSO) was appointed from within the security office.

In July 2020, Government Witness 1 (GW1), a GS-13 security professional, was hired as the PSO for a more senior program office with oversight authority of Applicant's SAPF. At hearing, there was considerable testimony about a series of non-alleged events that occurred shortly after GW1's hire in which she challenged Applicant and PMO leadership over the approval process for an information system that Applicant developed. Ultimately no security violation was found, but Applicant and witnesses agreed that this incident contributed to tensions between Applicant's cybersecurity team and the broader security staff, to include the Organization PSO and GW1, the PSO with oversight.

In December 2020 and January 2021, several events developed that led to the allegations in issue. Applicant was out of the office with COVID-19 for some period during this timeframe, with access only to unclassified email. As highlighted later, the timing and duration of Applicant's absence became a matter of some consequence at the hearing, as they impacted his accountability for some of the alleged failures to perform his duties. During the adjudicative process, Applicant equivocated both on when he started sick leave due to COVID and when he returned to the facility.

Regarding the start date of his absence, Applicant submitted into evidence a written statement that he was out of the office **prior** to a hard drive crash on December 21, 2020,[1] that resulted in the loss of critical data in issue in the case. Applicant Exhibit (AE) X at 7-8. At hearing, however, Applicant testified that he was present when the hard drive crash occurred. Transcript (Tr.) at 758. Regarding the date that he returned to work, Applicant initially testified that he was out "well into January," but later testified that he was "out the month of January effectively into February, at least put into a position where I could only work from home" and "was not able to reenter the building until middle of February." Tr. at 334, 752-53. When confronted with evidence that he returned no later than January 28, 2021, Applicant wavered but acknowledged that he did return to the facility in late January. Tr. at 812-13; GE 4 at 1. Applicant's witnesses stated variously that he was out for approximately two weeks in January 2021 and that he returned to the office in mid-to-late January. Tr. at 713; AE F at 6. Given the conflicting testimony, the Judge suggested to Applicant that he might submit documents that would establish the dates of his absence, but Applicant failed to do so.

In February 2021, GW1 learned that Applicant was serving as media custodian. She informed the Organization PSO that Applicant should not be both the media custodian and ISSM because it represented a conflict of interest — "the whole purpose of an insider threat program is to make sure that your media custodian doesn't have the privileges that an ISSM would have." Tr. at 45-46. At about the same time, the Organization PSO discovered that Applicant had committed a security infraction, and she facilitated the appointment of PMO security office personnel as media custodians. By memo dated February 23, 2021, the Organization Program Manager at the time (PM1) appointed a security office member as media custodian and two others as alternate media custodians, including the Organization PSO.

In March 2021, after security personnel took over media custodian duties from Applicant, they "discovered systemic failures to comply" with the Service's controlling guidance for SAPs. Government Exhibit (GE) 6 at 2. Upon this discovery, the Organization PSO, with PM1 concurrence, asked the oversight PSO, GW1, to conduct an independent assessment of media control processes and documentation within the SAPF. Her assessment, conducted in April 2021, identified multiple discrepancies in how media in the SAPF were identified, controlled, and documented, and recommended corrective actions. GW1 forwarded her assessment to PM1 by memorandum dated May 3, 2021. GE 6; GE 7.

Upon receipt of GW1's independent assessment, the Organization ordered an in-house preliminary inquiry and assigned a contractor as preliminary inquiry officer (PIO). His report was completed in June 2021 and identified approximately nine areas of concern, largely mirroring GW1's assessment. GE 8. In July 2021, the Organization PSO forwarded the preliminary inquiry report to the Service's SAP central office (SAPCO). She had previously, in May 2021, forwarded the reports of two other inquiries into comparatively minor infractions by Applicant that had come to light earlier in the year. By letter of August 6, 2021, the SAPCO suspended Applicant's SAP access. GE 10.

[1] In the first inquiry into Applicant's performance of duties as media custodian, Applicant reported that he lost critical data due to a hard drive failure and identified the failure as occurring on December 21, 2020. GE 7 at 1.

The SOR reflects the issues and incidents documented in the three preliminary inquiry reports submitted to the SAPCO. Broadly speaking, Applicant asserted that the following factors accounted for the alleged security discrepancies: poor record-keeping by the predecessor media custodian; lack of training as media custodian; lack of an approved SAPF standard operating procedure (SOP), resulting in varying interpretations and conflicts between program personnel; initial lack of access to SAPF safes to inventory any media they contained; poor relations between security personnel and his cybersecurity team; and unfair targeting by the Organization PSO. On this final assertion, Applicant and his counsel repeatedly cited to the fact that the Organization PSO submitted the preliminary inquiry reports directly to the SAPCO, rather than sending them through the chain of command for endorsement. Applicant also questioned the impartiality of the in-house preliminary inquiry of June 2021 (GE 8), suggesting that the PIO was improperly influenced by the Organization PSO. Notably, the Organization leadership — both PM1 and his successor PM2 — supported Applicant in his assertion that he was unfairly targeted by the PSO. AE SS; AE TT.

Security personnel who testified, including GW1, GW2, and GW3 (the Program Executive Office Director of Security and the Organization PSO's senior rater), voiced a markedly different viewpoint. They attributed tensions between the Organization PSO and Applicant to Applicant's lax attitude towards compliance with security regulations, his unwillingness to provide requested information, and his negative attitude towards particular security personnel. They testified that the Organization PSO was required to forward the preliminary inquiries to the SAPCO, notwithstanding the Organization concerns. GW3 testified that, upon her review of GW1's assessment and the three preliminary inquiries, she found the findings and conclusions were supported by the evidence and that the inquiries were consistent with common practices. Tr. at 226-29. Several security professionals attested to retaliation or harassment against PSO and others for investigating and reporting Applicant's suspected security infractions.

SOR Allegations in Issue

SOR ¶ 1.h: *From at least December 2020, until at least March 2021, Applicant failed to properly maintain media logs as required by his position as designated media custodian*. The Judge identified this allegation as the most significant issue of security concern. His lengthy findings of fact are incorporated in the summary below.

According to the SAPCO's Insider Threat Implementation Guidance, issued in May 2016, the media custodian is required to maintain a media log in accordance with a particular template, which requires the following data: Media Control Number - Type of Media - Date Entered Control - Date Issued - Name of Person to Whom Issued - Purpose of Issue - Data Transferred - Session Opened - Session Closed - Transfer Activity Verified - Media Disposition - Date of Disposition.

Essentially, the media custodian is required to control and track all removable media (*e.g.*, CDs and DVDs) from cradle to grave — from its entry into the SAPF until its destruction. Upon removing its original wrapping (*e.g.*, a spindle of CDs in plastic wrap), the media custodian is required to number all discs and enter the numbers and the date into the media log. When issuing media, the media custodian must update the media control log to identify the person to whom the media was issued, the purpose of the issue, the date/time of issue, and the number of files being transferred. After the data transfer is complete, the media custodian must: 1) receive and review the media to

verify that the number of files transferred matches the original log entry; 2) ensure destruction of the media using approved methods when no longer required; and 3) update the log accordingly. Media logs are normally maintained on a computer network or handwritten on a paper log.

Within the SAPF, personnel designated as data transfer agents (DTAs) conduct all file transfers and are responsible for securely moving, reviewing, and sanitizing data across different security domains or classification levels. When the media custodian issues a CD or DVD to a DTA, he also gives the DTA a data transfer questionnaire. After the DTA conducts the data transfer, the DTA returns the media and a completed DTQ to the media custodian, who verifies the number of files on the media and disposition information. That is, in addition to the media control log, which tracks all media from issuance of a media control number through destruction, each piece of media is tracked with its own DTQ. The eight DTQs in evidence were one-page hard copy documents filled in by hand. AE W.

Both GW1's independent assessment and the subsequent in-house preliminary inquiry established that **no** media control logs existed for the period in which Applicant was media custodian. Upon inquiry by GW1 in April 2021, Applicant stated that the media control logs were lost due to hard drive failures on two different workstations on August 20, 2020, and December 21, 2020. GE 7 at 1. In her assessment, GW1 noted that Applicant did not report the failures until March 22, 2021, "when security personnel were reconciling historical media documents," and she questioned the report of the earlier failure on August 20, 2020, as security office records "reflect the replacement hard drive for that workstation failure was brought into accountability 24 June 2020." *Id*. During the subsequent preliminary inquiry, Applicant again cited "multiple system crashes" to explain the lack of a media control log or database. GE 8 at 2.

In response to the SOR, Applicant repeated his assertion that workstation failures were to blame but also asserted that he had recreated, at least in part, the lost media control log:

> Media logs were maintained in accordance with established policy and procedures. . . . However, in or around January of 2021 the primary computer used to store the logs and associated media disposition forms suffered a hardware failure. Despite efforts to recover the system, all files and records were lost including the media logs. All available historical documentation – to include paper copies of media forms – were used to support recreation of the media logs to as accurate a level as possible. Despite those efforts, there were several pieces of media for which logs could not be regenerated.

Answer at 8.

Over the course of the three-day hearing, Applicant was questioned repeatedly about this critical issue — whether he created and maintained the required media control log and, if so, what happened to it. Applicant testified as follows regarding his initial efforts and the first crash: when he assumed duties as media custodian in March 2020, he created an Excel spreadsheet with all the required data fields; he maintained the digital log on a stand-alone workstation on a particular information system (IS1) because his requests for access to a backed-up network were denied; the hard drive on that workstation crashed in August 2020, and he lost the media log; over the course of a week or more, he then re-created the digital log on two information systems (IS1 and IS2) and

populated the data fields with information derived from paper DTQs. He again maintained this digital log on a stand-alone workstation because he did not have access to the shared drive.

Regarding the subsequent December 2020 hard drive failure, fundamental questions emerged during the hearing, including whether Applicant was present when the failure occurred and — to some extent — whether it actually happened. In a written statement submitted prior to the hearing, Applicant stated that the "hardware failure occurred while [he] was out of the office due to a severe bout of COVID." AE X at 7-8. At hearing, however, he testified that it occurred shortly before he was out with COVID, when a colleague was imaging Applicant's hard drive from his stand-alone computer to migrate the data to a third information system (IS3). Tr. at 544, 751. Applicant stated that his colleague "was sitting like right next to me" when the system went down. *Id*. at 757-58. In response to questions from the Government about whether he reported the failure, Applicant stated that he did report it, but he failed to produce any corroboration. Tr. at 814. The Judge highlighted to Applicant that the record did not include a statement from this colleague to corroborate that there in fact was a second hard drive failure in December. Applicant responded, "I can get that to you," but he did not do so. Decision at 10 (citing Tr. at 757-58).

Applicant testified repeatedly and in specific detail that, after the December 2020 crash, he recreated a digital Excel media control log from DTQs, that it was on both IS2 and IS3, that he turned the logs over to security when they assumed media custodian duties, and that security's claim that there were no logs was "just unequivocally false and untrue." Tr. at 740. He identified two program security personnel who could attest to the existence of the logs but called neither as a witness nor submitted statements from them. Applicant also testified that AW1, the ISSM for IS3, could "attest . . . to the existence of those logs on [IS3]." Tr. at 545-47.

When AW1 testified on direct examination, he stated that Applicant maintained media logs on a spreadsheet consistent with SAPCO guidance until a hard drive failure in about August 2020 and that there were media logs on IS3 for media issued from August 2020 to February 2021, when the duties were transferred to security. Under cross-examination, however, AW3 acknowledged that, although he believed that he had seen a media log for the period prior to August 2020 in a spreadsheet format similar to the prescribed template, he had **not** seen a media control log on IS3 for the period from August 2020 to February 2021, he did not believe that such a media log existed on the system, and there were only scanned copies of DTQs on IS3.

On the third day of the hearing, after AW1 and other witnesses testified, the Judge again asked Applicant what he did to recreate the media control log after the December 2020 hard drive failure, and he acknowledged for the first time that he in fact had **not** recreated the media control log:

> I was not given the opportunity beyond uploading the DTQs. . . . All I was able to do given the sickness, given the investigation, given the series of meetings that we had to talk about the discrepancies. . . . The reconstitution of the logs would have occurred on [IS3]. . . I uploaded all the scanned DTQs into [IS3]. My next stop would have been to .reconstitute those logs to the best of my ability on [IS3], which was a fully compliant backed up solution.

Tr. at 766-67.

In his colloquy with the Judge, Applicant asserted that he "consider[ed] the DTQs to be substantive for, you know, for the logs necessary to recreate for the media custodian." *Id*. at 773. He ultimately acknowledged, however, that it was not "a one for one match" and that a DTQ is "a form that has data that could be used to create a log" but is not itself a log. *Id*. At the end of their dialogue, Applicant admitted, "I did not give them a log due to the failures. I gave them DTQs and the media that I had." *Id*. at 775.

Applicant testified that he distributed approximately 60 pieces of media during the time he was media custodian. He submitted eight DTQs into evidence, primarily in response to an allegation no longer in issue. Applicant testified that AW1's team was trying to obtain copies of additional DTQs scanned to IS3, but he did not submit any additional DTQs prior to the close of the record. Decision at 13. Regarding Applicant's claim that DTQs include the same information as a media log and could be used to recreate a log that complied with SAPCO requirements, the Judge found that DTQs include "much but not all data required to be maintained in a media log"; that the DTQs in evidence were not equivalent to a media control log and "include insufficient information to determine if there is an insider threat problem"; and that "[t]wo of the eight DTQs in evidence do not include information essential to a media log (one fails to identify where data was transferred to (i.e. purpose), and another fails to identify the date and time of media disposition)." *Id*. at 14 (citing AE W at 1, 3).

In conclusion regarding SOR ¶ 1.h, the Judge found:

> No media logs exist for the entire timeframe Applicant served as [] media custodian. His claims that he maintained media custodian logs in a spreadsheet consistent with SAPCO requirements from February 2020 until a hard drive failure in August 2020 are corroborated in part by AW1's testimony. . . . Applicant's claims that he recreated and maintained media custodian logs in a spreadsheet consistent with SAPCO requirements after an August 2020 hard drive failure until a second hard drive failure in December 2020 are unsupported by other evidence.
>
> Applicant's claims he used available documents including DTQs to reconstitute a media log in a spreadsheet consistent with SAPCO requirements after a December 2020 hard drive failure and provided those logs to security are untrue. His belated admission that he did not provide security with media logs but instead provided digital copies of DTQs from August 2020 to February 2021 is corroborated by other record evidence. This allegation is established.

Id.

SOR ¶ 1.b: *In or around 2020 and 2021, while the designated media custodian, and without authorization, Applicant improperly issued bulk media for future use or for no specific purpose*. In his Answer to the SOR, Applicant denied this allegation, explaining that a designated media custodian is permitted to issue multiple (i.e., bulk) media if the purpose of issuance is tracked. At hearing, he testified that there were four information systems within the SAPF, that transfers between the various information systems each required a different CD, and that mission requirements sometimes dictated that multiple CDs need to be issued. When asked specifically about issuing multiple CDs for future use, Applicant responded that "it depends on what the

definition of future is" and that "bulk issuance of media for a future use . . . was subjective based on [his] understanding, interpretation of media [] policy and requirements." Tr. at 531, 541.

Government's witnesses (GW1 and GW3) confirmed that issuing bulk media for future use or for no specific purpose violates applicable regulations. GW1 acknowledged that regulations do not explicitly prohibit issuing media in bulk and that a media custodian can issue the number of media required to complete the job, but highlighted that issuing bulk media without a specific purpose violates SAPCO insider threat guidance because the media custodian would not know the number of files being transferred or what the media is being used for. Her independent assessment of April 2021 revealed "[m]ultiple incidents" of Applicant issuing media in bulk without a specific purpose. GE 7 at 3. GW1 testified that she was informed during her assessment that, if Applicant were to be gone, he would simply issue bulk media. As an example, GW1 highlighted that Applicant issued five CDs in March 2020 to a person who died shortly thereafter in June 2020. Applicant did not account for the CDs when the person died, and the CDs were apparently discovered during an inspection of the deceased employee's work area in about April 2021.

The subsequent preliminary inquiry confirmed GW1's findings, concluding that there were multiple instances in which Applicant issued media in bulk to DTAs without proper approval. Similarly, a separate preliminary inquiry found, after review of statements submitted by two DTAs, "it is apparent that [Applicant] issued blank media in bulk for convenience." GE 4 at 2. In finding adversely on the allegation, the Judge concluded that the evidence established that "Applicant issued bulk media for future use including for his convenience or for no specific purpose." Decision at 18.

SOR ¶¶ 1.d and 1.e: *In or around 2020 and 2021, while the designated media custodian, Applicant improperly failed to properly assign media control numbers to newly opened media (1.d); and improperly failed to verify whether all media within the secure space were properly assigned media control numbers (1.e).*

Because these allegations are so closely related, we address them in the aggregate. Applicant testified that, when he opened a new spindle of CDs, he would immediately number them and enter them in his digital media log and that two coworkers were in the room with him during this process. He did not submit testimony or statements from either coworker to corroborate his claims. During the preliminary inquiry, the PIO found that multiple CDs were discovered in the SAPF that were not marked with media control numbers. Citing to his lack of access to safes within the SAPF, Applicant asserted that he could not complete a full audit when assuming his media custodian duties and asserted that the unmarked CDs were issued by his predecessor. The PIO noted, however, that Applicant had failed to renew his request for access to the safes when a new PSO was appointed in December 2020.

As a separate issue, the Judge also highlighted that the eight DTQs in evidence confirmed that, although Applicant may have labeled those particular CDs, he did so improperly in that he did not use the media control number conventions specified in the controlling guidance. As a consequence, the "DTQs show that he issued multiple pieces of media with near-identical media control numbers and inconsistent media control number conventions." Decision at 21, 22. For both SOR ¶¶ 1.d and 1.e, the Judge concluded that "[e]ven assuming Applicant was unable to access

some security containers to verify all media in the SAPF, the available DTQs are sufficient to establish this allegation." *Id.*

SOR ¶ 1.f: *In or around 2020 and 2021, Applicant improperly allowed blank media, with assigned control numbers, to exist within the space without accounting for the discrepancies and their disposition.*

The June 2021 preliminary inquiry found that multiple CDs with control numbers were found throughout the SAPF, both in and out of safes, and that the media was not being tracked by the media custodian. In his response to the PIO, Applicant attributed this situation to "multiple system crashes and the lack of approval from security to inspect the security containers prior to new PSO assuming position in December 2020." GE 8 at 3. Moreover, and as discussed above, GW1 reported that Applicant issued five CDs to a coworker who died three months later, that Applicant did not account for the CDs when the person died, and that they were not discovered until inspection of the work area in April 2021. The Judge concluded that evidence was sufficient to establish the allegation.

SOR ¶ 1.g: *In or around [April] 2021, while the [ISSM], Applicant improperly allowed manufactured CDs to be introduced into the controlled space without being controlled.*

Applicant denied the original allegation, which did not allege a specific month and alleged "media custodian" vice "ISSM." Over Applicant's initial objection to amendment, the Judge provisionally granted the Government's motion to amend to develop the record. Tr. at 87-91. Based on the evidence presented at the hearing, the Judge noted in his decision that any remaining objection to the amendment was overruled.

The record includes evidence of two relevant incidents, both of which occurred after Applicant was relieved of media custodian duties and was serving solely as ISSM: 1) two un-opened packages of media were found by security personnel in an unlocked cabinet in the SAPF on April 21, 2021; and 2) manufactured media that accompanied encryption devices were found by security personnel on about April 28, 2021.

As to the first, during an after-hours inspection on April 21, 2021, security personnel found one un-opened spindle of CDs and one un-opened spindle of DVDs in an unlocked cabinet in Applicant's office in the SAPF. GW1 testified there is a requirement that any media that comes into a SAPF must be accounted for by the media custodian; that blank media may be referred to as "manufactured"; and that this media had not been brought to the media custodian for accountability as required by SAPCO guidance regardless of whether the media is wrapped or loose.

The Judge concluded that there was insufficient evidence to determine when the spindles of CDs and DVDs were introduced into the SAPF and whether Applicant was the media custodian at the time.

As to the second incident, the record evidence is cloudy. Applicant was apparently not present when encryption devices that he ordered were delivered on or about April 27, 2021, and placed in the SAPF, apparently at his direction. When security personnel entered the inventory space, they found opened boxes containing both encryption devices and manufacturer media, and they took possession of six CDs that had not been brought to security for accountability. Both GW1's

report and the subsequent preliminary inquiry highlighted that Applicant had given training in late February 2021 on SAPF media control requirements and that this chain of events was in contradiction of the protocols that he had outlined.

Both in his Answer to the SOR and at hearing, Applicant asserted that manufactured CDs, whether commercial software used by IT personnel or factory-sealed fresh media, are specifically excluded from media control requirements. Applicant testified that security is responsible for inspecting hardware that enters the SAPF and that security personnel introduced the encryption devices into the SAPF. He anticipated receiving only the encryption devices because they were being shipped from a military distribution center but acknowledged that security also found a manufacturer-sealed disc that contained drivers. The Judge concluded:

> It is unclear who initially inspected the package(s) containing the encryption equipment and who introduced the package(s) into the SAPF. It is undisputed Applicant was not present when encryption equipment was delivered on April 27, 2021. There is substantial evidence the manufactured CDs should have been brought to the attention of the then-media custodian/security personnel when introduced into the SAPF, that security personnel found "opened boxes containing [encryption devices and manufacturer media]" in the inventory space and that [security personnel] "confiscated six CD's that had not been brought to security for accountability." Applicant's claim that security found "a disc, a closed, manufacturer-sealed disc that contained drivers" is insufficient to refute evidence that Applicant was culpable for failing to maintain control of six manufacturer CDs found in "opened boxes," which had not been brought to security for accountability. This allegation is established.

Decision at 26-27.

Character Evidence and Applicant's Training

Applicant called five witnesses and submitted numerous letters of recommendation, including from a general officer, senior government civilian employees, current and former supervisors, colleagues, and friends. The witnesses and letters commented favorably on Applicant's integrity, trustworthiness, judgment, reliability, work performance, cybersecurity expertise, handling of classified and sensitive information, and commitment to national security.

Applicant testified that he requested but did not receive formal training for his media custodian duties prior to his appointment in March 2020. Applicant confirmed that he previously received extensive training on rules and regulations associated with the handling of SAP information and SAPFs, including annual training. As ISSM, he oversaw training of prospective DTAs, and he had previously served as a DTA with "burn privileges." Tr. at 458. Applicant also testified that, several years before being appointed as a media custodian, he "worked directly with media custodians . . . on a day-to-day basis [and] understood all their process, their policies, and their execution of their job functions."*Id.* He was "[v]ery familiar" with rules and regulations applicable to media custodian duties. *Id.* at 459. He recalled that, when SAPCO updated the Service's insider threat guidance in 2016, he was provided with relevant material and self-trained on the updated material. Additionally, Applicant acknowledged that he reviewed relevant policy

and procedures upon assuming the duties and that he received a rough draft SOP from his predecessor.

Matters Not Alleged in the SOR

At hearing, the Government inquired into a matter not alleged in the SOR — Applicant's disclosures on his November 2021 security clearance application (SCA) regarding the suspension of his SAP access. In the Employment Activities (Section 13A) portion of his SCA, Applicant disclosed that he was advised that incident reports had been filed against him and that physical access to the SAPF had been removed. However, in response to the question in Section 25: Have you EVER had a security clearance eligibility/access authorization denied, suspended, or revoked? Applicant checked "No." GE 1 at 15, 44. He testified that he answered "No" because he believed that the matter was still in adjudication and that a final decision had not been reached. Applicant also testified that his Facility Security Officer (FSO) recognized that his response was incorrect, that she gave him an opportunity to fix it, and that he ultimately corrected his response. Post-hearing, Applicant submitted an email chain with his FSO in which he discussed revising his SCA. The Judge found, however, that "Applicant submitted no documentary evidence he corrected his response to the SCA suspension question or that he certified and submitted a revised SCA." Decision at 34.

Judge's Analysis

For the six allegations detailed above, the Judge found that the evidence established AG ¶ 34(g) *any failure to comply with rules for the protection of classified or sensitive information*. As elsewhere in his decision, the Judge highlighted the singular importance of Applicant's failure to maintain the required media control log, as alleged in SOR ¶ 1.h:

> The record includes substantial evidence Applicant failed to properly establish and maintain accountability and control over media located in a SAPF while serving as media custodian, as alleged in SOR ¶¶ 1.b, 1.d-1.f, 1.h, and that as ISSM he improperly allowed manufactured media into the SAPF without it being controlled in SOR ¶ 1.g. Most significantly, no media log exists for the more than 11 months Applicant served as TPI media custodian. The lack of a media log raises significant questions about Applicant's performance of media custodian duties and complicates assessment of potentially mitigating conditions.

Id. at 37.

In his mitigation analysis, the Judge expressed "significant concerns about Applicant's credibility and judgment" for reasons that included, *inter alia*:

1) Applicant's testimony that he provided a media log in the form of "a digital Excel spreadsheet" upon being relieved as media custodian was untrue, and Applicant "confirmed the falsity of this testimony on the third day of the hearing";

2) Applicant's explanations for why he claimed to turn over media logs to security

personnel and why he claimed that security personnel lied about not receiving them were not credible for numerous reasons to include:

a. He lied about turning over an Excel spreadsheet media log;

b. He told contradictory narratives about whether the hard drive failure occurred on December 21, 2020, or in January 2021 and whether he was present or out with COVID when the failure occurred; and

c. His "persistent efforts" to equate a DTQ to a media log until the final day of the hearing "suggest an intent to deceive and/or raise significant questions about his judgment";

3) Applicant's testimony and demeanor at the hearing were "unconvincing and inconsistent with someone who was reliably telling the truth"; and

4) Matters not alleged in the SOR, specifically his differing explanations for failing to disclose his SAP access suspension on his November 2021 SCA, "raise additional credibility and judgment concerns."

Id. at 38-39.

The Judge acknowledged that the conduct in issue occurred over a period of less than a year and five or more years ago. However, he noted that "Applicant's failure to accept responsibility for his conduct undercuts a determination that he has reformed and rehabilitated himself." *Id*. at 41 (citation omitted). He concluded:

> As discussed above, I also have significant concerns about his credibility and judgment and his truthfulness at hearing. His failure to comply with rules for the protection of SAP information demonstrates a pattern of noncompliance or loose compliance with some rules based upon his interpretation of the rules and demands of his ISSM responsibilities. Notwithstanding that Applicant has held a security clearance over the past five years without engaging in any further security concerning behavior, there is insufficient evidence to support a conclusion the behavior is unlikely to recur and his conduct casts doubt on his current reliability, trustworthiness, and judgment.

Id.

In addressing Applicant's assertion that his lack of training on media custodian duties contributed to these alleged incidents, a mitigating circumstance under AG ¶ 35(c), *the security violations were due to improper or inadequate training or unclear instructions*, the Judge acknowledged that Applicant may not have received formal training prior to his appointment. He noted, however, that Applicant had "extensive SAP and SAPF experience, training and certifications" and that he had been an ISSM and a DTA. *Id*. at 42. The Judge also highlighted Applicant's testimony that he had worked closely in the past with media custodians, that he was very familiar with the applicable rules and regulations, that he understood their processes, their policies, and their execution of their job functions, and that he had "self-trained" on the updates to

DoD and Service insider threat guidance in 2016. With regard to AG ¶ 35(c), the Judge concluded: "[Applicant's] most significant security violation was his failure to properly maintain a media log, duties which are well defined in applicable directives including a requirement to maintain a media log in accordance with detailed sample. On balance, the evidence is insufficient to support a conclusion the security incidents were due to inadequate training. *Id.*

Whole Person Concept

In his Whole-Person Concept analysis, the Judge explicitly considered the following factors, among others: Applicant's strong character evidence and reputation as a cybersecurity professional; the lack of other security incidents; the training he received, including the lack of specific media custodian training; his inability to complete a full audit of media upon assuming media custodian duties; and the lack of evidence that any classified or protected information was compromised. He concluded:

> Despite the mitigating evidence presented, Applicant has not met his "very heavy burden" in demonstrating mitigation. ISCR Case No. 14-05127 at 8 (App. Bd. June 24, 2016). His false claim that he maintained a media log in a spreadsheet format and provided it to security when media custodian duties were transitioned and other credibility and judgment concerns detailed in the analysis section leave me with significant doubts about his credibility and judgment. And his failure to accept responsibility for all security incidents alleged in the SOR except for one (SOR ¶ 1.l) undercuts a determination that he has reformed and rehabilitated himself. *See* ISCR Case No. 96-0360 at 3-4 (App. Bd. Sep. 25, 1997). Notwithstanding that Applicant has held a security clearance over the past five years without engaging in further security incidents, I find that his security significant conduct continues to cast doubt on his current reliability, trustworthiness, and good judgment.

Id. at 43.

Discussion

On appeal, Applicant contends that the Judge "rest[ed] the entire decision on a single finding, that the records I preserved took the form of [DTQs] rather than adhering to the provided sample format, and on a finding that I had been less than truthful." Appeal Brief at 2. Specifically, he argues that "the dispositive ¶ 1.h finding is not supported by substantial evidence and rests on an arbitrary distinction between the form of a record and its security substance" and that the adverse credibility determination "misclassified a good-faith definitional dispute as a lie." *Id.* at 2-3. For the reasons detailed below, we are not persuaded.

Although the Judge explicitly identified Applicant's failure to maintain a media log (SOR ¶ 1.h) as "the most security significant conduct in this case,"[2] our review of his adverse decision confirms that it is grounded in his consideration of the entire record, to include Applicant's own testimony, the testimony of four witnesses called by the Government and five called by Applicant, and voluminous exhibits. After his exhaustive review, the Judge concluded that the Government

[2] Decision at 43.

established seven allegations and that Applicant failed to mitigate six of them. The Judge identified the conduct alleged in SOR ¶ 1.h as the most serious, but it was unquestionably not the sole basis for his decision.

We turn now to Applicant's assertions regarding SOR ¶ 1.h and the Judge's related credibility assessment, as we concur that those two issues are of primary importance in the Judge's resolution of this case. Applicant argues that SOR ¶ 1.h is not supported by substantial evidence and that the record instead "establishe[d] that the substance of media accountability existed and was recoverable, and that the only deficiency was one of documentary form." Appeal Brief at 4. This argument is inaccurate and misleading. The requirement for Applicant to maintain a media control log was indisputably established by Government witnesses, by policy directives that he submitted, and by his own admission. At the conclusion of the three-day hearing, it was also indisputable that no media control logs existed for Applicant's tenure as media custodian. Applicant now asserts that he "preserved and produced" all the required information in individual DTQs rather than a spreadsheet. *Id.* at 5. This argument fails for several reasons, but we will address three.

First, and to state the obvious, a collection of scanned pieces of paper filled out by individual DTAs is not the same as a comprehensive chronological log maintained by the media custodian and does not meet the requirement to maintain a log that is established by the SAPCO. Second, the DTQ forms in evidence lack many of the data fields required for the media control log, to include: the date the CD/DVD entered the SAPF, the files that were transferred by the DTA, the time that the transfer session opened and closed, and verification by the media custodian of the transfer activity. Third, Applicant failed to produce the DTQs that he asserted satisfied the requirement. Applicant testified that he issued about 60 pieces of media, but he submitted only eight DTQs into evidence. Although he testified about efforts to locate and submit additional DTQs, he failed to submit any or to request additional time to do so. Decision at 13. Upon review of the scant eight DTQs in evidence, the Judge found some were not even completely filled out: "Two of the eight DTQs in evidence do not include information essential to a media log (one fails to identify where data was transferred to (i.e. purpose), and another fails to identify the date and time of media disposition)." *Id*. at 14.

We turn next to the Judge's adverse credibility determination, which Applicant challenges as the Judge's mischaracterization of "a good-faith definitional dispute." Appeal Brief at 3. This challenge on a pivotal issue — whether Applicant was truthful during the investigative and adjudicative processes — falters under the sheer weight of the decision and the record that supports it. We note first that the Directive requires us to give deference to a Judge's credibility determination. Directive ¶ E3.1.32.1. A judge can personally observe a witness's demeanor when testifying and can form impressions about the credibility of that witness's testimony based on an assessment of his demeanor. "A party challenging such a credibility determination has a heavy burden of persuasion on appeal." ISCR Case No. 03-05072 at 5 (App. Bd. Jul. 14, 2005).

Here, the Judge did not hedge or waffle on his credibility assessment but instead explicitly stated, "I found [Applicant's] testimony and demeanor at the hearing to be unconvincing and inconsistent with someone who was reliably telling the truth." Decision at 39. We pause here to note that this was a three-day hearing during which Applicant testified for about six hours on Day Two and several additional hours on Day Three, giving the Judge a prolonged opportunity to assess

his demeanor under extended questioning by his counsel, Government counsel, and the Judge himself. In addition to his general assessment of Applicant's demeanor, the Judge highlighted specific statements that Applicant made as "contradictory," "untrue," or "false," including his differing narratives about when the purported second hard drive failure occurred and whether he was present, his testimony on Day Two that he reconstituted a media log in a spreadsheet consistent with SAPCO requirements after that hard drive failure, and his testimony that he provided a media log in the form of "a digital Excel spreadsheet" to the newly appointed media custodian when those duties were transferred to security in about February 2021. *Id*. at 14, 38, 43.

Under the Judge's questioning on Day Three of the hearing, Applicant finally "confirmed the falsity of this testimony" and admitted that he had not recreated a media log after the December 2020 hard drive failure and that he had not provided security with a media log, but had instead given them copies of scanned DTQs. Decision at 38. Applicant now seeks to characterize this exchange with the Judge as quibbling over a definition of a "log" and asserts that "the Judge resolved the definition with me on the record, and accepted my logic." Appeal Brief at 9. The transcript entirely refutes this assertion. It reveals that the Judge's lengthy colloquy with Applicant in the closing hours of the hearing was for the purpose of clarifying his confusing, misleading, and persistent efforts to equate the scanned DTQs to a media log. Contrary to Applicant's arguments, the record and specifically the transcript support the Judge's finding that Applicant lied about these matters. Decision at 39. Applicant has not met his "heavy burden of persuasion" to rebut the Judge's adverse credibility determination, and we decline to disturb it. Contrary to Applicant's argument, the Judge's material findings about SOR ¶ 1.h and his conclusion that the allegation was established by substantial evidence are amply supported by the record.

Other Errors

Applicant also alleges errors not associated with SOR ¶ 1.h, including: 1) that the Judge's Whole-Person determination "underweighted an exceptional record"; 2) that the Judge's mitigation analysis under AG ¶ 35(c) was contradicted by his own findings; 3) that the Judge gave unalleged conduct disqualifying weight; 4) that he "drew adverse inferences from an inquiry whose author the Government never produced"; and 5) that he amended an allegation over objection, undermining Applicant's prepared defense. Appeal Brief at 3. We find no merit in any of these allegations, which are discussed briefly below.

The Judge's Whole-Person Concept analysis reflects a thorough review and consideration of Applicant's strong character evidence, his reputation as a cybersecurity professional, his work on significant defense projects, his excellent reputation for reliability and good character, his recognized technical skills, and his sound record of performance. Applicant's ability to argue for a more favorable weighing of that record evidence is not sufficient to demonstrate that the Judge weighed the evidence in a manner that was arbitrary, capricious, or contrary to law.

Applicant argues that the Judge's findings of fact support application of AG ¶ 35(c) and that he erred in failing to apply this mitigating condition in light of his own findings. We disagree. In his findings, the Judge acknowledged a lack of formal training on Applicant's particular duties as media custodian but cited to his extensive SAP and SAPF experience and training and his admitted deep familiarity with the position and duties of media custodians, to include their processes and the governing DoD and Service policies. The Judge also explicitly found that the

duty to properly maintain a media log, which he characterized as the most significant security issue in the case, was well defined in the applicable directives. We find no contradiction between those findings and the Judge's ultimate conclusion that the alleged security incidents were not due to inadequate training and not mitigated under AG ¶ 35(c).

As to Applicant's assertion that the Judge gave unalleged conduct disqualifying weight, the decision clearly reflects that the Judge considered that conduct within the confines of the precedent to which he cited. Decision at 39. And as to Applicant's assertion that the Judge drew adverse conclusions from the preliminary inquiry (GE 8) without the PIO being produced, we note only that Applicant failed to object to the admission of GE 8 at hearing, obviating the need for any further discussion.

Finally, Applicant argues that the Judge amended SOR ¶ 1.g over objection, allowing the Government to allege that he was performing duties as ISSM rather than media custodian in April 2021, and thereby "defeated [Applicant's] prepared defense." Appeal Brief at 3. At hearing, Applicant's attorney objected to the proposed amendment with a caveat: "I'll object at this time . . . I'd rather wait until all the testimony is in to include [Applicant] so he can address it as well . . . because we're going to walk through each one of the allegations in the SOR." Tr. at 88. The Judge then "provisionally grant[ed]" the motion to amend. *Id*. at 91. Neither of the parties raised the matter again later in the hearing, and the Judge subsequently overruled the objection in his decision. To the extent that Applicant initially objected to the amendment, his qualified objection was remedied by what his counsel requested, a thorough examination on SOR ¶ 1.g at hearing, during which the topic of whether he was ISSM or media custodian at the time in issue was thoroughly explored. Moreover, the Judge held the record open for over a month, during which Applicant submitted additional materials. We are convinced that Applicant received the due process to which he was entitled regarding this amendment to the SOR.

As the Judge highlighted in his decision, security violations "strike at the heart of the industrial security program." Decision at 37 (citing ISCR Case No. 03-26888 at 1 (App. Bd. Oct. 5, 2006)). As the Appeal Board has previously discussed, most frequently applicants are denied a clearance because they have an indicator of a risk factor—such as drug use, alcohol abuse, or financial delinquencies—that raises a concern they **might not** comply with rules and regulations surrounding the protection of classified or sensitive information. *See* ISCR Case No. 03-26888 at 1. Here, the Judge found that Applicant, a person entrusted with safeguarding SAP information, **did not** comply with established requirements, and the record supports those findings. Our precedent establishes that an applicant in such cases has "a very heavy burden" of demonstrating that he should again be entrusted with classified information. ISCR Case No. 00-0030 at 6 (App. Bd. Sep. 20, 2001). The Judge concluded that Applicant did not carry that burden, and we concur.

Conclusion

Applicant has not established that the Judge's conclusions were arbitrary, capricious, or contrary to law. Rather, the Judge examined and weighed the disqualifying and mitigating evidence and articulated a satisfactory explanation for the decision, and the record is sufficient to sustain the Judge's findings and conclusions. "The general standard is that a clearance may be granted only when 'clearly consistent with the interests of the national security.'" *Dep't of the*

Navy v. Egan, 484 U.S. 518, 528 (1988). "Any doubt concerning personnel being considered for national security eligibility will be resolved in favor of the national security." AG ¶ 2(b).

Order

The decision in ISCR Case No. 22-02555 is **AFFIRMED**.

Signed: Moira Modzelewski
Moira Modzelewski
Administrative Judge
Chair, Appeal Board

Signed: Allison Marie
Allison Marie
Administrative Judge
Member, Appeal Board

Signed: Eric H. Borgstrom
Eric H. Borgstrom
Administrative Judge
Member, Appeal Board