DEFENSE LEGAL SERVICES AGENCY
DEFENSE OFFICE OF HEARINGS AND APPEALS

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

Appearances

For Government: Andrea Corrales, Esq., Department Counsel
For Applicant: Ronald C. Sykstus, Esq.

05/26/2026

Decision

PRICE, Eric C., Administrative Judge:

This case involves security concerns raised under Guideline K (Handling Protected Information). Eligibility for access to classified information is denied.

Statement of the Case

Applicant submitted a security clearance application (SCA) on November 10, 2021. On March 28, 2023, the Defense Counterintelligence and Security Agency (DCSA) sent him a Statement of Reasons alleging security concerns under Guideline K. The DCSA acted under Executive Order (Exec. Or.) 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; Department of Defense (DOD) Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the adjudicative guidelines (AG) promulgated in Security Executive Agent Directive 4, *National Security Adjudicative Guidelines* (December 10, 2016).

Applicant answered the SOR on April 19, 2023, and requested a hearing before an administrative judge. The case was assigned to me on June 10, 2024. On July 26, 2024, the Defense Office of Hearings and Appeals (DOHA) notified Applicant that the hearing was scheduled to be conducted via video teleconference on August 27, 2024. On

August 19, 2024, Department Counsel requested a continuance because of a medical issue with the Government's only witness. I found good cause for a continuance and over Applicant's objection approved Department Counsel's request. (Hearing Exhibit (HE) I) After consultation with counsel including reconciliation of witness availability, the hearing was scheduled for December 9-10, 2024. (HE II)

I convened the hearing as rescheduled using the Microsoft Teams video teleconference system. The hearing was conducted on December 9, 10 and 13, 2024. Department Counsel called four witnesses and Government Exhibits (GE) 1 through GE 11 were admitted in evidence without objection. (Transcript (Tr.) 22-27; HE III) Applicant testified, called five witnesses and offered Applicant Exhibits (AE) A through AE QQ. (HE IV) AE A, AE B and AE D through AE QQ were admitted without objection. I sustained Department Counsel's objection to AE C, an unsigned statement, and later admitted AE OO, a signed version of the same statement. (Tr. 308-311, 713-719) I kept the record open so the parties could submit additional documentary evidence. (Tr. 850-853) Applicant submitted AE RR through AE UU and Department Counsel submitted GE 12 and GE 13, which were admitted without objection. (HE V) DOHA received the transcript on December 27, 2024, and the record closed on January 29, 2025.

Findings of Fact

The SOR includes 12 allegations under Guideline K. In his answer to the SOR, Applicant admitted the allegations in SOR ¶¶ 1.c and 1.l, with explanations, and denied all other allegations with explanations. (SOR Response) At hearing, he expressed concerns about SOR ¶ 1.c, and I have treated his concerns as a denial of that allegation. (Tr. 433-34, 548-49) Applicant's admissions are incorporated as findings of fact.

Applicant is a 40-year-old cybersecurity lead employed by a defense contractor since September 2019. From December 2008 to September 2019, he was employed by other defense contractors in various information system administration and security positions including as a system and network administrator, communications security (COMSEC) officer, cybersecurity analyst and lead. He earned a bachelor's degree in management information systems and a master's degree in cybersecurity. He has obtained multiple certifications including Certified Information System (IS) Security Professional. He was engaged to be married at the time of his hearing and co-parented his fiancée's four children. He has held a security clearance since 2008. His Special Access Program (SAP) access was suspended by a service SAP central office (SAPCO) in August 2021. (GE 1, GE 10, GE 11 at 5; AE F, AE X; Tr. 315-24, 414, 794-795)

In September 2019 Applicant was assigned as a contractor employee in a program management office (PMO) for a military organization (organization) under a program manager (PM1). At the time, the organization had no in-house cybersecurity team, and the PMO was standing up a special program office. Applicant was brought in to support cybersecurity requirements and IS capabilities. His primary duties were as IS Security Manager (ISSM) and included responsibility for ensuring PMO IS and information technology (IT) compliance with SAP regulations. (GE 1; AE H, AE U, AE X; Tr. 45-46)

In about March 2020, Applicant was also appointed as the two-person integrity (TPI) media custodian (hereinafter media custodian) for several IS in a SAP facility (SAPF) that supported the PMO. (AE U, AE X) Media custodian duties had previously been performed by security personnel or contractors but assigned personnel requested to be relieved of those duties. Applicant reluctantly accepted and protested being assigned as the "'lone media custodian' because he did not want to be a single point of failure[.]" (AE X at 10; Tr. 355) He was selected for this role in part because of his outstanding reputation for mission-accomplishment and professional knowledge. Duties as media custodian include establishing control of media upon entry into the SAPF and accountability for all such media until destruction in accordance with applicable regulations. His primary office and the SAPF were in the same building about five minutes walking distance apart. (Tr. 454-71, 708-09, 721-32; AE H)

Applicant's media custodian duties required frequent interaction with security personnel including the program security officer (PSO). PSOs manage the security, compliance, and access for SAPs including enforcement of policies, approval of access, management of SAPF physical security, and oversight of classified document control. (Tr. 31, 346, 453, 515-517) The working environment in the secure spaces including the SAPF was described as fast paced and affected by professional and personal conflicts. (GE 11; AE H, AE SS-TT; Tr. 96-97, 119-128, 156-160, 199, 237-38) Applicant had a good relationship with some security personnel but not with others including PSO1 and PSO2. He initially had a good personal and professional relationship with PSO2, but the relationship deteriorated after PSO2 was appointed as PSO with responsibility for the SAPF in December 2020. (GE 11; AE H, AE SS-TT; Tr. 447-49)

In July 2020, Government Witness 1 (GW1), a GS-13 security professional was hired as PSO for a program office with oversight authority over the PSO for the program Applicant supported. (Tr. 31, 42-51, 130-131; AE H at 3, AE M at 4) When GW1 reported aboard there was tension between Applicant, PMO leadership and security personnel over an IS developed by Applicant. Security personnel including GW1, PSO1, and PSO2 believed: Applicant had not provided requested paperwork; he misrepresented that the IS had been granted authority to operate (ATO); he was operating the IS on a SAP system before receipt of an approved ATO constituted a potential security violation; and they sought to shut the system down pending investigation. These tensions culminated in a contentious meeting between program stakeholders and representatives of other organizations and contributed to tensions between Applicant and some security personnel. (GE 11, GE 13; Tr. 32-44, 404-05, 420-21, 570-74, 593-97; AE H, AE X at 5-6, AE UU) At the time, there was an approved change request for the IS but not an approved ATO. Ultimately no security violation was found, and the IS was permitted to continue operating. (Tr. 70-71, 404-06, 571-74; AE TT)

Applicant testified PM1 and PM2 (program manager of another program in the PMO, senior SAPF leader, and Applicant's primary point of contact for SAPF matters) said he "did a fantastic job", the SAPCO said "this is fine", and that he received a "commendation from [his employer]" because program leadership said "[he] did a great

job." Applicant testified that if he "did not do the appropriate documentation" for the IS he "would not have kudos. I don't even know if I'd have a job." (Tr. 405, 462-63) After the hearing he submitted a statement from PM2 confirming there was no security violation and noting that after the contentious meeting they developed a plan to get the final ATO approved. PM2 informally counseled Applicant because he failed to submit final ATO paperwork after previously being asked to follow up on it. PM2 counseled Applicant not to let it happen again and stated Applicant told him COVID hit shortly after their change request had been approved, and the final paperwork "fell through the cracks." (AE TT)

Applicant was out of the office with COVID-19 from late December 2020 until mid-to-late January 2021 or February 2021. (SOR Response; Tr. 334, 710-12; AE F at 6) He said he was out "well into January" and later said "out the month of January effectively into February, at least put into a position where I could only work from home. I was not able to reenter the building until middle of February." (Tr. 334, 752-53) A friend and colleague who worked closely with Applicant estimated he was out for "approximately two weeks" in the January 2021 timeframe. (Tr. 700-13) Applicant's Witness 1 (AW1), Applicant's friend and SAPF colleague, stated he returned to the office in "the mid-to-late January timeframe." (Tr. 113; AE F at 1-6, AE X) While working remotely Applicant only had access to unclassified email and a telephone. (Tr. 764-65) I expressed interest in documentary evidence to determine how long he was out of the office with COVID and Applicant said he could probably submit emails or time sheets but did not do so. (Tr. 756-57, 775-76)

In February 2021, after learning Applicant was serving as media custodian, GW1 informed PSO2 that he should not be both the media custodian and ISSM because the "purpose of the insider threat program is to make sure that your media custodian doesn't have the privileges that an ISSM would have." (Tr. 45-53, 143-45, 217-219) Around the same time, PSO2 determined Applicant committed a security infraction and facilitated the appointment of program security office personnel as media custodians. (GE 4 at 1-2) By memo dated February 23, 2021, PM1 appointed a program security office member as media custodian and two others as alternate media custodians including PSO2. (AE U) The exact date media custodian duties were transferred to security is unclear. Applicant contends duties were transferred on February 23, 2021, and memos from April and May 2021 state media custodian duties were transferred in March 2021, and on March 8, 2021. (Tr. 365, 431, 440, 488, 556; GE 6 at 2, GE 7 at 4, GE 8 at 1)

In March 2021, after media custodian duties were transferred, security personnel "discovered systemic failures to comply with [SAP] Insider Threat Program Guidance." (GE 6 at 2) PSO2 with PM1 concurrence requested GW1 assess media control documentation and processes. GW1 forwarded her review to PM1 by memorandum dated May 3, 2021. (GE 6-7) The review identified discrepancies in media control documentation and implementation of SAP insider threat guidance, and recommended corrective actions including that PM1 address the discrepancies before an Inspector General (IG) visit scheduled for September 2021. (GE 6-7; Tr. 150-152)

From April 28 to July 29, 2021, three preliminary inquiries were conducted by program security personnel into 12 suspected security incidents attributed to Applicant and forwarded to SAPCO. (GE 2-5, GE 8-10) Most matters addressed in the preliminary inquiries had been noted in GW1's review and forwarding memo. (GE 6-7)

Most SOR allegations relate to Applicant's duties as media custodian and allegedly occurred while COVID-19 protocols were in effect. Applicant asserted his lack of media custodian training (notwithstanding his requests), and the lack of an approved SAPF standard operating procedure (SOP) resulted in varying policy interpretations and conflicts between program personnel. (Tr. 362-63, 782-94) He cited a fast-paced working environment, constrained timeline, lack of experience and personnel turnover as contributing to strained relationships between security and cybersecurity. He said his predecessor media custodian provided incomplete records and that security concerns prevented him from auditing all media in the SAPF. Specifically, he said PSO1 and PSO2 denied or ignored his requests for access to some safes and rooms or to audit media stored therein because he lacked the required clearance or need-to-know certain information or cited a lack of security staffing. (SOR Response; AE X at 9-10, AE NN, AE QQ at 4; Tr. 338-40, 354-56, 389-91, 460-78, 551-63, 623, 733-39, 761-63, 782-94)

Applicant also alleged PSO2 unfairly targeted him and expressed concerns about the investigative process and reporting to SAPCO and DCSA. He cited tensions with PSO2 including her history of escalating matters, avoiding accountability, and influence over others involved in the inquiries. He suggested PSO2 made good on threats to get his security clearance revoked even if she had to manipulate evidence. (SOR Response; AE X; Tr. 347-49, 410-15, 489-94, 792-94) Several witnesses attested to a personality conflict between Applicant and PSO2, PSO2's inappropriate comments about getting security clearances revoked or suspended (though most thought she was joking at the time), that some of her past allegations were unfounded, and that PSO2 sometimes elevated security concerns if displeased with initial results. (Tr. 240-41, 335-37, 412-14, 562-66, 624-26, 633-43, 702-05; AE F, AE H at 3-4, AE OO, AE SS, AE TT)

PM1 and PM2 believe that PSO2 "targeted" Applicant. (AE SS-TT) PM1 opined PSO2 "used all tools available to her to resolve the situation in an unfair manner" and stated at least three investigations into SAPF security incidents raised by PSO2 and GW1 came back unfounded including an investigation of PM1 himself. (AE SS) PM1 also noted:

> none of the security incidents [in the program], including [Applicant's], resulted in impacts to National Security [and stated] a couple of [Applicant's security] incidents . . . came down to interpretation of [service] Regulations [to determine] if a security violation occurred. In these cases, I had the security team document the incident, then contact [SAPCO] for guidance. [SAPCO] determined that some incidents were violations and other incidents resulted in updated policies. This process of always documenting events is partially why [Applicant] and others had security incident memos, but not all memos turned into security violations. (AE SS)

PM2 stated that after counseling Applicant and PSO2 about unprofessional workplace behavior, Applicant modified his behavior but that PSO2 had not. PM2 disagreed with the conduct of the inquiries and with some findings. PM2 opined GW1 unnecessarily exacerbated PSO2's security concerns and that PSO2 sometimes saw issues where none existed. (AE TT)

Applicant and PM2 challenged the accuracy of a key preliminary inquiry, GE 8. Applicant testified that he discussed the preliminary inquiry with his friend and its author, contract security specialist (CSS). Applicant said CSS initially thought the preliminary inquiry "had it right" but after being informed there were policy disputes and reviewing the policy CSS concurred with Applicant's assessment. (Tr. 490, 521) PM2 stated that CSS said he "would not have written the report the way it was written" but was directed by PSO2 "to change the words in the report to make [Applicant] look bad." (AE TT at 3) GW3 testified CSS provided a statement in a "formalized inquiry" stating he had been asked to discredit PSO2, to report PSO2 had been "targeting [Applicant]" and that "these security infractions . . . weren't as bad as they sounded [and] were being reported because [PSO2] had some sort of personal vendetta against [Applicant]." CSS "refuse[d] to oblige" the request and did not believe the derogatory statements about PSO2 were accurate. GW3 cited details from CSS's statement, but this statement is not in evidence. GW3 noted the inquiry found no fault with PSO2's handling of matters involving Applicant. (Tr. 230-32) Notably, GE 8 was admitted into evidence without objection, Applicant's and PM2's statements do not identify or contradict any specific finding in GE 8, and GW's testimony directly contradicts most of their assertions. Applicant did not call CSS as a witness or submit a statement from him.

Security personnel including GW1, GW2, and GW3 (program executive office director of security and PSO2's senior rater) attributed tensions between PSO1, PSO2 and Applicant to Applicant's lax attitude towards compliance with security regulations, unwillingness to provide requested information and his negative attitude towards some security personnel including PSO2. (Tr. 105-125, 158-59, 177-82, 199-202) GW3 reviewed most of the preliminary inquiries and GW1's assessment and thought the findings and conclusions were supported by the evidence and that the inquiries were consistent with common practices. (Tr. 226-29; GE 2, 4, 6-9) PM2 confirmed PSO2 expressed concerns about losing her security clearance because of SAPF security issues. (AE TT) PSO2 expressed concerns to her supervisors about retaliation from Applicant's supporters including PM1 and PM2 for investigating and reporting his suspected security issues. Several security professionals attested to retaliation or harassment against PSO2 and others after the suspected incidents were reported. (Tr. 105-109, 190-92, 200-205, 229-38; GE 11)

I find GW1, GW2, and GW3's testimony that PSO2 was required to forward preliminary inquiries regarding incidents involving SAP to the SAPCO, notwithstanding PM1's or PM2's concerns, credible. (Tr. 122-25, 156-57, 188-93, 221-28; GE 6-7) I also find GW3's testimony that SAPCO personnel advised PSO2 to enter the security incidents into a DCSA information system after learning no reports had been entered to be credible. (Tr. 221-26; SOR Response; AE H) Given the evidence of tensions between Applicant

and PSO2 and GW1, PSO2's inappropriate comments about getting his security clearance revoked or suspended, and contradictory claims regarding the fairness of the investigative process and accuracy of the various inquiries, I will conduct a thorough review of the evidence pertaining to the SOR allegations. I will address SOR ¶ 1.h first because it also relates to other allegations.

SOR ¶ 1.h: From at least December 2020, until at least March 2021, you failed to properly maintain media logs as required by your position as designated media custodian. Applicant denied the allegation.

SAPCO Insider Threat Implementation Guidance states "**The TPI Media Custodian shall maintain a removeable media log IAW the sample template provided** in Enclosure 1 to Enclosure 4."[1] (AE CC at 2 subparagraph e.(1))[2] (emphasis added) The "Sample TPI Media Log" includes 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. The "Sample TPI Media Log" also provides a "Media Control Number" numbering convention starting with a number and year ("01-2013" and "02-2013") and "Type of Media" samples ("CD-R" and "DVD-R"). (AE CC at 3) The media control log is used "to record all removeable media data transfers and retain the logs on file for audit purposes." (AE CC at 2) SAPCO promulgated that "[b]ased on Insider Threat risk assessments, the [SAP] community faces the greatest security risk from information system users, particularly those with privileged status." (AE AA at 2) Organizations are required to "develop and implement an Assured File Transfer (AFT) [SOP]." (AE AA at 3)

A media custodian is required to number all media and enter the numbers and the date the media entered control into a media log immediately upon removal of original wrapping. When issuing media, the media custodian should update the media control log to include name of person to whom the media was issued, purpose of the issue, date/time of issue and number of files being transferred. The media custodian will receive and review media upon completion of data transfer to verify the number of files transferred matches the original log entry and to ensure destruction of the media using approved methods when no longer required and then update the log accordingly. (Tr. 51-52, 141-43, 434-40; AE AA at 4, ¶3(e)(2)(c-f), AE CC at 3)

Applicant described media custodian duties as "extremely important" and including any SAPF IS that is allowed for an AFT of information, accounting for all media brought under control, marking it accordingly and maintaining a chain of custody associated with the media with a log to back that up "cradle to grave." (Tr. 739) Media logs are normally

[1] The "Sample TPI Media Log" submitted by Applicant and admitted in evidence without objection is "Enclosure 1 to Enclosure 3" vice "Enclosure 1 to Enclosure 4." (AE CC at 2-3) The Insider Threat Implementation Guidance dated October 23, 2013, includes three enclosures and Enclosure (3) is "TPI Procedures," therefore, the reference to "Enclosure 1 to Enclosure 4" appears to be a scrivener's error. I consider the "Sample TPI Media Log" in evidence to be authentic. (AE CC at 3)

[2] Applicant misidentified the Insider Threat Implementation Guidance dated October 23, 2013 as AE DD vice AE CC. (Tr. 352, 431, 743; AE CC, AE DD)

maintained on a computer network or on paper or in a handwritten log. (Tr. 255-56, 758-59) Applicant decided to maintain a media log on IS1, a Top Secret network because he wanted to use an available network that was regularly backed-up and because his predecessor as media custodian requested that he do so. (Tr. 758-62) A media log is normally unclassified but takes on the classification of the IS it is stored on until declassified. (Tr. 748) GW3 was unaware of a requirement to backup media logs. (Tr. 255-56)

A data transfer agent (DTA) conducts AFTs and is responsible for securely moving, reviewing, and sanitizing data across different security domains or classification levels. A data transfer questionnaire (DTQ) is provided by the media custodian to the DTA, who fills in most fields. After the DTA conducts a data transfer, the DTA fills in the remainder of the DTQ and brings it and the media back to the media custodian who verifies the number of files on the media and disposition information. The eight DTQs in evidence are scanned copies of forms filled in with handwritten information and are discussed in detail under SOR ¶ 1.c. (AE W; Tr. 583-86, 745-47; GE 7 at 1)

A preliminary inquiry conducted by CSS (a subordinate of PSO2) found that prior to security personnel taking over as media custodian in March 2021:

> there is no previous Media Control Database on record. [Applicant] explained no Media Control Database exists due to multiple system crashes. No Media Control Database was rebuilt from latest system crash on December 21st 2020 until the March 2021 timeframe [when the new media custodian established one]. At this current time no Previous Media Control logs exist on record prior to March 2021. See References A [Applicant's MFR dated June 2, 2021] & B [Applicant's MFR dated March 23, 2021 "Subject: Media Custodian/Disposition Logs – Data Loss"].

(GE 8 at 1-2; GE 6, GE 7 at 1)

GW1's assessment and report noted "No incoming media logs were maintained as required" by insider threat guidance. (GE 7 at 1, 2, 4, GE 6) Applicant reported losing historical media control logs due to hard drive failures on different workstations on August 20, 2020, and December 21, 2020. (GE 6, GE 7 at 1) The assessment questioned the date of the August 2020 hard drive failure "because the actual replacement hard drive for that workstation was brought into accountability 24 June 2020 . . . before [Applicant] said it failed and he lost his data." (GE 7 at 1; Tr. 68-69)

In response to the SOR Applicant explained that:

> 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. A Memorandum for Record (MFR) was created to document this event, and accompanied the documentation transitioned to the cognizant security authority . . . during the change of media control duties.

(SOR Response at 8)

Applicant testified he made a digital copy of the "template for a media log" from the insider threat guidance which he stored on IS1, and "had a physical copy that [he] maintained in conjunction with the [DTQs]." (Tr. 352) He used "the sample template" media log from the Insider Threat Guidance to create "an Excel spreadsheet" and kept it on a standalone workstation on IS1 from January 2020 until August 2020. (Tr. 351-52, 740-48, 820) His three requests for access to an automatically backed up network shared drive were denied by PSO1 and PSO2, who cited concerns about granting him access to a drive with information he was not authorized to access. (Tr. 344-47, 515-21, 734-39) He said the media log and other disposition records were lost when the hard drive failed in August 2020 because it was not backed up to a shared drive. (Tr. 345-52, 740-48) After the August 2020 hard drive failure, he tried to manually duplicate the records based on information pulled from paper records including DTQs. (Tr. 517-19) "I had some written down. Like I mentioned [the DTQs] were fairly extensive so they included a lot of the documentation and data that comes from that needs to be included on the media log. . . . So, I maintained a digital media log that was in the same templatized format as the one that I showed you and the [DTQs] had the requisite data to fill that out." (Tr. 517-18)

Applicant claimed that after the August 2020 hard drive failure he "recreate[d the media logs to] the best of my ability based on all the information we pulled from the paper records." (Tr. 518) He said that he manually duplicated the records and "created a digital log on [IS1 and IS2] because I didn't have access to the shared drive on [IS1]. My back up strategy was trying to manually duplicate the records on [IS1 and IS2]. But it wasn't long after that that PSO2 took over the media custodian duties and I handed over everything I had." (Tr. 517-19) He estimated it took him a week or more to recreate the media log from DTQs and other available information after the August hard drive failure. (Tr. 811-12) The standalone local workstations were not backed up because they were top secret. He was frustrated and angered by the loss of his "media custodian logs because [security] wouldn't give [him] access to the shared drive [which he conveyed via email]." (Tr. 344-47, 515-21, 737, 810-12)

Applicant testified he maintained the media log "in accordance with policy and procedures, but in January [2021] the computer hard drive did crash. I then took the [DTQs] that I had on paper for them, and provided them . . . to reconstitute the logs to the best of my ability. In February when the transition of the media custodial duties was done, I handed all those logs over to [PSO2 and security]." (Tr. 440-41; SOR Response at 8) In a written statement, he indicated the hard drive "failure occurred while [he] was out of the

office due to a severe bout of COVID" but testified that it occurred shortly before he was out sick with COVID and believed that it occurred on December 21, 2020. (AE X at 7-8; Tr. 521, 544-45, 750) A preliminary inquiry citing two MFRs from Applicant indicates a hard drive crash occurred on December 21, 2020. (GE 8 at 1-2) He testified that the hard drive failure occurred when a colleague was imaging his standalone computer's hard drive on IS2 while attempting to migrate the data to IS3. (Tr. 750-52) I informed Applicant the record did not include a statement from his colleague, and he responded "I can get that to you" but did not do so. (Tr. 757-58)

Applicant testified he maintained or recreated media logs from paper copies including DTQs and turned them over to security. (Tr. 347-50, 435-36, 517-21, 544-45) He said that he recreated the logs as best he could "in January [2021]" and then created a digital version that he transferred to security in February 2021. (Tr. 544-45) "As soon as I came back [from COVID], I tried to fill out the media custodial log to show TPI accountability. Right? [The DTAs] had destroyed one of the disks, which you know, I can't maintain the log if they've destroyed the disk, so I can't [show disposition]. So I wrote an MFR to [PM2], [PSO2] and others assigned to security[.]" (Tr. 755-56; AE GG) In a written statement he indicated that he "attempted to recreate the media control logs based on paper logs but had limited time and resources to perform the action before media control was turned over to security[.]" (AE X at 8)

In response to questions about why an investigation determined no database was rebuilt from December 2020 until March 2021 Applicant responded "There wasn't a database. . . . It was just a digital Excel spreadsheet. I provided that to [the newly appointed media custodian from security]. It was on [IS2 and IS3]." (Tr. 544-46, 820) Claims "that there were no logs and that I did not transfer over any logs to Security. That's just unequivocally false and untrue. I literally have Exhibit W, that shows DTQs." (Tr. 740) He asserted the "problem is that the source [PSO2] tainted the information. . . . I did give security media logs, because I did keep them manually. I had data transfer questionnaires, the DTQ's they mentioned. I was able to rebuild those logs. And I provided it to security." (Tr. 347) "[A]t that time it was transitioning over so what I did was, I took the digital logs that I had . . . on the other system. I had reconstituted the majority of the logs from . . . the paper DTQs. And I scanned them in and I submitted them all to security[.]" (Tr. 521)

Applicant testified AW1, as ISSM for IS3, "could attest . . . to the existence of those logs on [IS3]." (Tr. 545-47) He also identified two program security personnel who could attest to the existence of the logs, including the security specialist he transferred media custodian responsibilities to and CSS. (Tr. 544-48) Applicant did not call his successor as media custodian or CSS as witnesses or submit a statement from either.

On direct examination AW1 testified Applicant maintained media logs "on a spreadsheet using the format that's outlined in the Insider Threat Policy Guidance" until a hard drive failure in about August 2020. (Tr. 569) He said that after hard drive failures in August and December 2020 "there are logs on [IS3] . . . media logs for media that was issued from August to, I think, up to February, when the media custodian duties

transferred over to security." (Tr. 569) During cross-examination, AW1 acknowledged he had not seen a media log in IS3 for the period August 2020 to February 2021. He believed he had seen a media log for the period prior to August 2020 in "spreadsheet format, very similar to the template that's prescribed in the example that they give you from the insider [threat] policy." However, for the period from August 2020 to February 2021, he saw only scanned copies of DTQ's and confirmed Applicant uploaded those files. (Tr. 583-88) "[AW1 did not] believe there's a spreadsheet media log on [IS3]. I think it's just, it's just the scans of the DTQ's." (Tr. 587)

In January 2024, AW1 wrote Applicant "provided [security] all available historical artifacts to allow for recreation of the lost logs [and] [i]t is accurate to state that upon media custodian role transition no consolidated media log existed, and that it had to be recreated from historical documentation." (AE F at 6) He believed Applicant scanned DTQ's onto the shared IS while updating the media log to ensure redundancy in case of another failure based upon his discussions with Applicant. (Tr. 601-607; AE F at 6)

Applicant testified a DTQ includes essentially the same information as a media log, "it maps out, especially on outside transfers every single field that's filled out in that form maps to the -- the requirements by SAPCO." (Tr. 741-42) The DTQs "included a lot of the documentation and data that . . . needs to be included on the media log." (Tr. 517-18) AW1 testified a DTQ captures everything required in a log and that he would think it would satisfy SAPCO policy requirements for a media log. (Tr. 601-607) AW1 testified:

> So for all intents and purposes, the DTQ's can be seen as the log . . . it's just not in a spreadsheet format. . . . So the insider threat policy has a sample template that most programs use. . . . It's an Excel spreadsheet that . . . you can use to input the data for your media logs. But everything that's [in] those fields are also transferred in the DTQ's. So the information is there. Now, there was not a spreadsheet associated with all of those DTQ's. That was not there. But the source files for them are there.

(Tr. 586-87)

AW1 testified that maintaining media logs from DTQ's is "not a best business practice" and asserted "spreadsheets . . . are a little bit more of an effective way to do it. But you know, if the purpose is to meet the intent of the policy, I would argue that the DTQ's meet the intent of that policy." (Tr. 585-88, 605-07) When asked how DTQ's could be a reasonable substitute for a media log required by the SAPCO, AW1 responded:

> all of the pertinent information in the insider threat policy is captured on the DTQ's. The other thing is the example template that's provided is just that, it's an example template. There's no requirement for organizations to use that template. It's really just a sample of hey, this is what we think this should look like.

(Tr. 605)

In her assessment, GW1 recommended attempting "to recreate a historical media log using the [DTQs] on [IS3], which were uploaded August 2020 to February 2021." (GE 7 at 1) The DTQs "could be used to recreate [a media log] as much as possible." (Tr. 72) The DTQ's provide "derivative documentation to re-create the log" and provide some historical data but "we . . . couldn't track the media as far as what number are you on, what's the title, how many logs, etc. and then you really -- without these media logs you don't know if you have an insider threat problem." (GE 7 at 1; Tr. 68, 83) GW1 did not see media logs created by Applicant or recreated from the DTQ's. (Tr. 51-77, 134-38)

After AW1 testified, Applicant was asked what he did to recreate the media log after the December hard drive failure and responded: "I would say that -- I was not given the opportunity beyond uploading the DTQs. We scanned -- 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 step would have been to reconstitute those logs to the best of my ability on [IS3], which was a fully compliant backed up solution." (Tr. 766-67) He then said the media distributed at the direction of PM2 and PSO2 while he was out sick with COVID was the only media transfer conducted after the December hard drive failure until media custodian duties were transferred. (Tr. 766-68) The following colloquy occurred shortly thereafter:

> [Administrative Judge] Okay, now, earlier, you indicated that the people were not being completely honest with respect to what they discovered in their investigation. Help me understand what's not honest, because now you're referring to the government exhibits with respect to there being no media logs during that time period, specifically. So what did you mean?
>
> [Applicant] So it was my understanding that there was some log that was transitioned over, but now that we've discussed, the, as you've heard from [AW1's] testimony, right, and mine, I consider the DTQs to be substantive for, you know, for the logs necessary to recreate for the media custodian. But I understand security's point that they're saying they didn't.
>
> If they're trying to say they didn't receive logs, my interpretation, understanding of that accusation was we didn't give them. Because they, because they said that to us. They said we gave them nothing.
>
> [Administrative Judge] I'm not going to parse words with you here, but the distinction between the log and a document that's a backup document is, I'm not sure we need to. Are you telling me that you think providing DTQs equals providing logs?
>
> [Applicant] I do not believe that that constitutes. I agree with you, Your Honor. Like, I don't think it's a one for one match. It's a form that has data that could be used to create a log. It is not a log.

> [Administrative Judge] Okay, that's a distinction with [a] difference. But I understand your position and I understand your testimony that you were using the DTQs to reconstitute. There were no further transfers. And at the time you transferred over to [security] you actually provided the DTQs, which in your mind means that you provided some information from which a log could be recons[tituted].
>
> [Applicant] Yes, Your Honor.
>
> [Administrative Judge] Okay. I understand and I'm not disputing the logic of that, but the difference between a log and a document that includes most of the information you would have in a log does not equal [a] DTQ, [and a DTQ] does not equal a log.
>
> [Applicant] **I understand that distinction now.** . . . I agree that explicitly I was taking the accusation to mean we did not give them anything based on conversations and emails where it stated that we didn't give them anything. The accusation states no incoming media logs, you know, were provided. So I understand the distinction. We did give them the DTQs. I was hoping that I could support them and help that transition to help reconstitute the logs with that . . . to support the transition of duties. . . . And I wanted to provide them all the necessary evidence…necessary artifacts and documents to support that transition. **I did not give them a log due to the failures. I gave them DTQs and the media that I had. So I do understand the distinction**.

(Tr. 772-75) (emphasis added)

Applicant testified that over the entire time he served as media custodian he distributed approximately "60 or so" pieces of media. When he took over as media custodian:

> the spindle that they gave me was partially exhausted and it really had very minimal left. I unwrapped and marked an entire full spindle . . . which was 50. And like the DTQ -- so obviously we're having an extremely hard time pulling them off of the Secret SAR information system, but I did speak with the administrators of [IS3] and they do have records from like the time period that's cited I failed to do my duties to show . . . here are DTQs. . . . And the number that they said was consistent with what I believed to be, like 60 or so. (Tr. 749)

Applicant testified AW1 and his team were trying to obtain copies of DTQs scanned to IS3 and working with security to approve the export of those logs or DTQs. (Tr. 749-50) However, he did not submit any additional DTQs or request more time to do so.

Applicant's claim that a DTQ includes essentially the same information as a media log and could be used to recreate a media log that satisfies SAPCO requirements is corroborated in part and refuted in part. A DTQ may be used to substantially re-create a media log because it includes much but not all data required to be maintained in a media log by the media custodian. However, a DTQ includes derivative documentation prepared by a DTA, not the media custodian, and the DTQs in evidence do not show the number of logs, the number of media entered into control or when the media was entered in control and include insufficient information to determine if there is an insider threat problem. Notably, in his SOR response, Applicant acknowledged there were several pieces of media for which logs could not be regenerated from historical documentation including DTQs. 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). (AE W at 1, 3)

No media logs exist for the entire timeframe Applicant served as TPI 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. However, available evidence shows that, at a minimum, he did not use the "Media Control Number" or "Type of Media" conventions specified in the Sample TPI Media Log. 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.

SOR ¶ 1.a: In or around 2020 and 2021, while the designated media custodian, you failed to verify and/or log virus scans on incoming media. Applicant denied this allegation.

Applicant acknowledged that virus scans are required to be performed on incoming media and asserted automatic organizational virus scans conducted on media inserted in organization IS after media was issued satisfied virus scan requirements. During his time as media custodian this was accomplished via tracking of information system ATO documentation that required malicious code protections under DoD risk management policies. He acknowledged that he did not conduct virus scans on incoming media prior to issuing it to DTAs. He asserted that logging of virus scans for incoming media is not required. (SOR Response at 2-3; Tr. 350-51, 428-31, 530, 795-810; AE-X at 8)

SAP insider threat guidance requires media custodians to "[e]nsure all incoming media is scanned for malicious code," and SAP organizations are required to "[s]can all

media upon issue by the TPI media custodian with an authorized antivirus product when initially connected/re-connected to an information system." (AE AA at 4 ¶¶ (1)f and (2)a) The DoD Joint SAP Implementation Guide (JSIG) requires organizations to "employ malicious protection mechanisms at [IS] entry and exit points to detect and eradicate malicious code [including] "real-time scans of files . . . as the files are downloaded, opened, or executed." (AE BB at 6)

A preliminary inquiry dated June 30, 2021, found "no records on file to ensure virus scans were being performed" and noted Applicant stated "information systems perform virus scans on media by default." (GE 8 at 2 citing Applicant's MFR dated June 2, 2021)

In April 2021, GW1 concluded media scans were not conducted as required and noted there was not a current SOP for media scan requirements. (GE 6, GE 7 at 2) GW1 testified she had not asked Applicant for proof automated scans were performed and acknowledged automatic virus scans would satisfy requirements for scanning incoming media when initially connected to or reconnected to an information system. Regulations do not require media custodians to log completion of virus scans on incoming media. (Tr. 51-53, 73-74, 133-36, 246-49; AE AA) GW3 confirmed the ISSM runs reports on what has been introduced into the system and was responsible for virus scans on the system. (Tr. 246-49) PM2 and AW1 confirmed media was automatically scanned upon insertion into a system computer and PM2 stated he was unaware of any program office doing a separate virus scan on newly opened media. (AE TT, AE F at 6-7; Tr. 33)

Automatic virus scans run when media was initially connected or reconnected to an IS satisfied JSIG and SAP insider threat virus scan requirements. As ISSM, Applicant was aware of and responsible for virus scans run on the system. As media custodian he was not required to log virus scans on incoming media. This allegation is decided for Applicant.

SOR ¶ 1.b: In or around 2020 and 2021, while the designated media custodian, and without authorization, you improperly issued bulk media for future use or for no specific purpose. Applicant denied this allegation explaining:

> Issuance of multiple (i.e., bulk) media is not prohibited by policy; official appointment as a media custodian authorizes the designated individual to issue media – no further authorization is required nor stipulated. "Purpose of issuance" is required to be tracked, and a media form was created and utilized for this purpose. The media form accompanied the media upon issuance and was used to update the media log.
>
> Data Transfer Agents (DTAs), at times, need to move data between multiple security domains requiring multiple media. Additionally, mission requirements often dictate the issuance of multiple media to meet deadlines or minimize operational impacts. Additionally, during this period I was the only designated media custodian supporting the office, and therefore a single point of failure. This issue was raised to management but was not

> rectified until February 23, 2021, when the role of media custodian was transferred to the cognizant security authority and two security support staff members. This resulted in several occasions where critical milestones were at risk, and media had to be issued in my absence.

(SOR Response at 2-3)

Applicant testified a media custodian can issue bulk media, but "you cannot issue it without a purpose." He denied issuing media without a purpose, said you have to record the purpose, and provided examples such as an "assured file transfer" or "move data from SIPR to NIPR to SIPR." (Tr. 477-78) He said that issuance of more than one CD was necessary because there were four IS and a transfer on each IS required a different piece of media. (Tr. 353) When asked about issuance of bulk media for future use, Applicant responded "I guess it depends on what the definition of future is, so the way . . . I did it was if someone requested the media to be used to make a burn I provided it to them, with the expectation that there was an expedience to it[.]" (Tr. 531) He was unaware of a requirement that "prohibits, or where it limits or identifies the span of time in which media has to be used." (Tr. 534) He believed "bulk issuance of media for a future use . . . was subjective based on [his understanding of] media policy and requirements." (Tr. 541) He said in the absence of an SOP and training he followed insider threat guidance and the JSIG and was unaware of any definition of future use. (Tr. 351-53, 477-79, 530-44; AE BB, AE CC; GE 6-8)

Applicant's written statement was consistent with his SOR response and included the following additional information:

> In fact, there are multiple instances where it may be necessary to issue multiple media due to separate classification levels or the inability of the media custodian to be available. As long as the media issuance and disposition are tracked, the requirements are fulfilled from a media custodian position. From a best practice perspective, it is not something that should be leveraged out of convenience, but rather from a point of mission requirement when no other alternative exists . . . in one instance when bulk issuance of media was required to support mission requirements, I was not available due to being out sick with COVID. [PM2 and PSO1 overrode my objection] for that issuance which supports my position that bulk media issuance was a known and accepted practice under the circumstances that existed at the time.

(AE X at 8-9)

Applicant testified:

> So if one developer needed to transition media or disposition of records to three different sources, he needed three CDs. So it was very common for me, especially not even sitting in the space, to say, okay, I'm going to come

> in, I'm going to issue you three to four CDs, you're going to do your job, I'm going to note the disposition of it, it's in your safe. I'm going to give you media control, you know, CD 1, 2 and 3. . . . And then that's the issue of purpose is, they're doing a file transfer to NIPR, to SIPR, to [IS1]. So it's absurd to say that there's no specific purpose. I have it documented. It's in their records. It's at [organization].

(Tr. 353)

A preliminary inquiry into another security concern noted after review of MFRs submitted by the two DTAs "it is apparent that [Applicant] issued blank media in bulk for convenience." (GE 4 at 2) A second preliminary inquiry found:

> There were multiple instances where Media was issued in Bulk for various reasons. [Applicant] stated that permission was granted by proper channels for the issuing of bulk media due to mission requirements as of January 2021. PSO/PM issued approval for a one-time mission requirement for this instance. Prior to January 2021 no approval for issuing of Bulk media can be found on record. Prior to January 2021 there are multiple instances where personnel were issued media in bulk. [Three DTAs] stated that they were issued media in bulk for future use or as needed on multiple occasions[.]

(GE 8 at 2)

GW1 reported: "Multiple incidents of [Applicant] issuing media in bulk while executing media custodian duties without a specific purpose documented in email as well as statements provided by [organization] personnel in violation of [various directives]." (GE 7 at 3) In March 2020, Applicant issued five CDs to a person who died in June 2020. Applicant did not account for the CDs when the person died, and the CDs were apparently discovered during inspection of the deceased person's work area in about April 2021 and turned over to security. (Tr. 81-83; GE 7 at 5-6)

GW1 testified media custodians are required when issuing media, "to update the media log to include name of person to whom the media was issued, purpose of the issue, date/time of issue and number of files being transferred. What I was told was that [Applicant] was busy [or] was gone and so before he would leave, he reportedly, according to the statements that I reviewed at the time, he would just issue bulk media and that's why blank media was found throughout the SAPF." (Tr. 75) GW1 reviewed "a series of statements" regarding bulk issuance of media. Bulk issuance of media makes it difficult to properly control or document media control. GW1 could not determine how long the bulk issuances occurred because there was no media log. (Tr. 74-77; GE 7 at 5-6)

GW1 acknowledged regulations do not explicitly prohibit issuing media in bulk, and said a media custodian can issue the number of media required to complete the job, but noted a specific purpose is required and that the media custodian must document the

number of files to be transferred. Issuing bulk media for future use 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. (Tr. 136-39) The "Sample TPI Media Log" and May 2016 SAPCO Insider Threat Implementation Guidance substantially corroborate GW1's testimony. (AE CC at 3, AE AA at 4 at ¶ 3.e.2.d)

GW3 confirmed media custodians are not authorized to issue bulk media for future use or no specific use. (Tr. 249-50) She testified there was a one-time approval for bulk media issued to two DTAs in January 2021. However, the DTAs "indicated that this is something that had been going on prior to them gaining that authorization, that it was really the way they operated, that they would get a couple of disks at a time instead of one at a time." GW3 confirmed issuing bulk media without a specific purpose is a violation of applicable regulations. (Tr. 217-18)

AW1 testified issuing bulk media "was a common occurrence within that space . . . . Every time it was issued, the DTA had to provide a justification for why they needed that number of discs." (Tr. 588) He said bulk transfers were not uncommon "in spaces that [he] work[s] in now[.]" (Tr. 588-89) He would be surprised if two DTAs said Applicant had given them bulk media for no particular purpose in the event they needed it in the future and said that was inconsistent with interactions he heard between Applicant and DTAs. (Tr. 589) Insider threat and other implementation guidance do not address bulk distribution; it is typically addressed in a facility SOP which was not developed until about 2023. (Tr. 610-11)

At least three DTAs stated they were issued media in bulk for future use or as needed on multiple occasions, and Applicant stated he would commonly issue additional media for convenience and mission accomplishment (if a DTA said "he needed three CDs. So it was very common for me, especially not even sitting in the space, to say, okay, I'm going to come in, I'm going to issue you three to four CDs"). After consideration of the testimony, available references and other evidence including Applicant's SOR Response, I find that the testimony of the government witnesses, and Applicant's admissions constitute substantial evidence that while designated media custodian and without authorization, Applicant issued bulk media for future use including for his convenience or for no specific purpose. Applicant's claim that on "several occasions where critical milestones were at risk, and media had to be issued in [his] absence" raises additional concerns because the record shows approval for only one such issuance (when he was out sick with COVID in January 2021). This allegation is established.

SOR ¶ 1.c: In or around 2020 and 2021, while the designated media custodian, you improperly issued, verified and/or signed for, multiple documents and media with duplicate media control numbers. Applicant admitted this allegation in his response to the SOR; however, I have treated concerns he expressed about this allegation at hearing as a denial. (Tr. 433-34, 548-49)

The eight media control numbers listed in GW1's review are identical to DTQ's Applicant submitted into evidence. (GE 7 at 4; AE W; Tr. 79, 142-80) A preliminary inquiry found that:

> multiple documents and media on record that contain the same media control numbers. Applicant stated there were duplicates of media control numbers due to the improper controlling of media from the previous media custodian before him and improper marking of documentation by users. There are multiple discrepancies with [Applicant's] statement. There are multiple records on file that contain duplicate media control numbers which were verified and signed by Applicant during his time as Media Custodian. See references A & F.
>
> (GE 8 at 2)

The final report of this incident prepared by PSO2 and submitted to the service SAPCO states "Supporting documentation show[ed] duplicate media was issued by [Applicant] during his tenure as Media Custodian." (GE 9 at 1) The supporting documentation was not submitted by the Government.

AW1 reviewed IS3 for DTQ's with apparently duplicate numbers to assist Applicant. He retrieved eight DTQ's, verified the documents were unclassified, and provided them to Applicant who submitted them into evidence. (Tr. 585-86, 768-70; AE W) "Those were the only duplicates that [AW1] could identify from just looking at the media controlled DTQ's that existed." He said "typically, you would see a standardized numbering system . . . C001, or D001 if it's a DVD. What I noted in this case was you had C0, you know, 020 and CD0020 . . . different batches of media that were numbered with similar numbering systems, which is quite a cause for confusion. Definitely not a best business practice." (Tr. 607-09; GE 7 at 4; AE W, AE F at 7-8)

The eight DTQ's were dated between July 14 and October 22, 2020, while Applicant was media custodian. (AE W) The media control numbers are very similar but not identical including, CDØ27 and C027, CD028 and C028, CDØ3Ø and C0030, C0045 and C045. He issued C0030 on July 14, 2020, C027 and C028 on July 22, 2020, CD028 on July 22, 2020, CDØ27 on August 31, 2020, C0045 on September 25, 2020, CDØ3Ø on October 1, 2020, and C045 on October 22, 2020. None of the media was disposed of on the date of issue except perhaps for CD028 which includes the DTA's initials next to "destroy", but the date/time of disposition are not identified. (AE W at 3) The DTQ for CDØ27 appears to omit the system the media was "transferred to" which Applicant previously provided as an example of recording the purpose. (AE W at 1; Tr. 477-78) Four of eight DTQs were disposed of more than 30 days after issuance. (AE W at 2, 4-5, 7) Applicant apparently signed or initialed four of eight DTQ's. (AE W at 4-8, AE TT at 2)

Applicant acknowledged that the better practice attested to by GW3 (using the media control number convention specified in the sample media log) would have reduced potential duplication. He claimed media with duplicate control numbers which he was

made aware of or identified were documented to ensure tracking and accountability. (SOR Response at 4-5; Tr. 354-56, 459-66, 488-89, 770-72; AE X at 9-10)

Applicant failed to use "Media Control Number" and "Type of Media" conventions specified in the Sample TPI Media Log. The media control numbers, and type of media conventions shown in the available DTQs were nearly identical, inconsistent, and confusing. Eight pieces of media with nearly identical media control numbers were issued and at least seven were disposed of while Applicant served as media custodian. This allegation is resolved for Applicant because the media control numbers are not identical.

SOR ¶ 1.d: In or around 2020 and 2021, while the designated media custodian, you improperly failed to properly assign media control numbers to newly-opened media. Applicant denied this allegation explaining that all newly-opened media provided to or unsealed by him "was assigned a media control number, labeled, and added to the media control log." (SOR Response at 5)

A preliminary inquiry found there

> were multiple CDs discovered that did not contain media control numbers. [Applicant] states that any media that was not labeled was due to the previous media custodian's improper handling of media when he took over, as well as the inability to access all security containers to verify any media within the containers. New PSO appointed December 2020, [with] no attempt by [Applicant] to verify any media within the space has been attempted. See Reference A [Applicant's MFR dated June 2, 2021].

(GE 8 at 2-3)

Applicant stated that he accepted the media custodian role contingent on support from security that never happened. "Without the appropriate and requested documentation, access to audit, and willingness to support I was unable to perform a complete transition of roles and responsibilities." He "documented every piece of media that [he] had access to, established a new media log, and labeled the unused media on the opened spindles that were provided in accordance with policy." He stated a full audit including all safes was not performed until security resumed media custodian duties:

> During that audit, additional media was discovered that had not been controlled. [PSO2 blamed me] despite the lack of access and multiple requests to perform audits. The complete misuse of power and redirection of blame shows a focus more on an emphasis to target someone maliciously to damage their character and career versus focusing on following processes and procedures to protect DoD information.

(AE X at 10)

Applicant testified consistently with his SOR Response and written statement. He said there was no evidence showing examples of media with improperly assigned media control numbers and that media still in its original wrapping was not required to be assigned a media control number. (Tr. 434-36, 549-53). He also testified:

> whenever I would unwrap that spindle, I sat in the room with two other people, [Coworker1] and [Coworker2], they would literally watch me like label it. It would be a spindle of 50 typically, because I really didn't want to do 100. . . . And so I would number them at that moment. And when I would do that, I would also create the digital log that was like hey, this is the new spindle . . . if anyone did their due diligence and actually went to the SAP to get the information and asked even for -- it's all unclassified . . . it's on the [IS3], it's on that system where those media records were controlled. Were they 100% accurate? No, because of the data drive that was lost, but because of my paper copies I was able to recover as much as possible and put it on those logs, but you would be able to see where I wrote CD one through 50. (Tr. 434-36)

Applicant testified AW1 and his team were trying to obtain copies of DTQs scanned to IS3 and working with security to approve the export of those logs or DTQs. (Tr. 749-50) However, he did not present testimony or submit statements from Coworker1 or Coworker2 to corroborate his claims, and he did not submit any additional DTQs or request more time to do so.

The preliminary inquiry and DTQs provide substantial evidence to support this allegation. SAPCO data transfer guidance specifies "[u]se only CD-R/DVD-Rs for data transfer and ensure they are properly labeled[.]" (AE CC at 2, ¶ 5.f.(5)) Applicant did not use the "Media Control Number" or "Type of Media" conventions specified in the Sample TPI Media Log and DTQs show that he issued multiple pieces of media with near-identical media control numbers and inconsistent media control number conventions. (AE CC at 3, AE W; Tr. 250-51, 355-56) Even 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.

SOR ¶ 1.e: In or around 2020 and 2021, while the designated media custodian, you improperly failed to verify whether all media within the secure space were properly assigned media control numbers. Applicant denied this allegation explaining:

> To the best of my knowledge, all media provided to me by the organization and media introduced during my appointment as media custodian were handled in accordance with applicable policy. . . . I was not permitted access to conduct a media audit on several Safes within the space. Lack of adequate supporting staff and need-to-know were cited as the reasons for denying this request. . . . Additionally, there was confusion and dissention between various parties within the organization regarding the policies

> governing media control. This continued after media custodian responsibilities had transitioned from me. For example, in March of 2021, a factory-sealed CD was discovered. The then appointed media custodian(s) insisted it needed to be controlled IAW policy.

(SOR Response at 6)

Applicant testified consistently with his SOR Response. He opined the allegation may refer to unused and sealed factory media and to manufacturer-sealed media sometimes provided along with equipment that is exempt from tracking and controlling by the media custodian. He cited SAPCO insider threat guidance and the JSIG as supporting authorities. (Tr. 436-38)

A preliminary inquiry reported:

> Multiple spindles of sealed uncontrolled media w[ere] found in the cyber security office. [Applicant] stated that he was unaware of any media being in the cyber security office. He stated that everything should have been transferred to [PSO2] when she took over as media custodian. [AW1] stated that the Spindles of media were found when the cyber security team were unpacking boxes of supplies for their office after their office went through construction of new furniture around 19th April 2021, which was then found by Security a few days later. [AW1] states that the media was simply overlooked during this unpacking process and must have been from the previous media custodian that was missed during handoff. See Reference A & C [Applicant's MFR dated June 2, 2021 and AE P].

(GE 8 at 3)

GW1 testified the only media her review identified with improperly assigned media control numbers was the media with duplicate media control numbers addressed in SOR ¶ 1.c. (Tr. 141-46; AE W)

The preliminary inquiry and DTQs provide substantial evidence to support this allegation. Applicant did not use the "Media Control Number" or "Type of Media" conventions specified in the Sample TPI Media Log, and DTQs show that he issued multiple pieces of media with near-identical media control numbers and inconsistent media control number conventions. (AE CC at 3, AE W; Tr. 250-51, 355-56) Even 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.

SOR ¶ 1.f: In or around 2020 and 2021, while the designated media custodian, you improperly allowed blank media, with assigned control numbers, to exist within the space without accounting for the discrepancies and their disposition. Applicant denied this allegation explaining:

> Blank media with assigned control numbers are allowed to exist within a SAP space under the control of the media custodian . . . . Further, blank media would inherently not be assigned a disposition until it was utilized.
>
> To my knowledge, all blank media was stored in the SAP space under the control of the media custodian as required by policy. This media is typically CDs and DVDs, which are purchased in spindles usually containing fifty (50) to one-hundred (100) individual discs. Upon removal of the spindle packaging, every disc included in the spindle was assigned a control number; and that control number was reflected in the media log.

(SOR Response at 6-7)

Applicant testified consistently with his SOR Response and asserted it is the media custodian's job to mark media once its original wrapping is removed with a media tracking control number before it is issued. He said the only part of the allegation he denied was the word "improperly" and asserted his procedures complied with applicable rules. (Tr. 439) He attributed discovery of media he had not accounted for to his lack of knowledge some media existed because he had not been briefed on its existence and because his requests for access to or audits of multiple rooms and safes had been denied. (Tr. 353-56, 438-40)

A preliminary inquiry found:

> Multiple CDs with control numbers were found throughout the [SAPF] (both in security containers and out) by multiple personnel that were not being tracked by the media custodian. [Applicant] states this issue is due 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. [Applicant] provided an MFR for these discrepancies for unknown documentation and disposition. No walkthrough of the space or inspection of the space was conducted between [Applicant] and [security personnel] when the transfer of media custodian occurred in March of 2021. See Reference A B & D [Applicant's MFR dated June 2, 2021, MFR re Media Custodian/Disposition Logs dated March 23, 2021, and MFR re Issuance of CDs to execute low risk AFTs dated April 19, 2021].

(GE 8 at 3)

As indicated previously, GW1 reported that in March 2020, Applicant issued five CDs to a person who died in June 2020. He did not account for the CDs when the person died, and the CDs were apparently discovered during inspection of the deceased person's work area in about April 2021 and turned over to security. (Tr. 81-83; GE 7 at 5-6)

The preliminary inquiry and GW1's report provide substantial evidence to support this allegation. Even assuming Applicant was unable to access some security containers to verify all media in the SAPF, evidence he issued five CDs to a person who died in June

2020 and that those CDs were not discovered or accounted for until about April 2021 is sufficient to establish this allegation.

SOR ¶ 1.g: In or around [April] 2021, while the [ISSM], you improperly allowed manufactured CD's to be introduced into the controlled space without it being controlled. Applicant denied the original allegation, which did not allege a specific month and alleged "media custodian" vice "ISSM." Over Applicant's objection I provisionally granted Department Counsel's motion to amend the allegation by substituting the words "around [April] 2021, while designated [ISSM]" and deleting the words "media custodian." (Tr. 87-91) Based on the evidence presented at the hearing, Applicant's objection to the amendment is overruled.

The record includes evidence of two relevant incidents: (1) two un-opened packages of media found by security personnel in an unlocked cabinet in the SAPF on April 21, 2021, and (2) manufactured media that accompanied encryption devices found by security personnel on about April 28, 2021. The incidents are discussed in order below.

A preliminary inquiry found:

> Multiple spindles of sealed uncontrolled media [were] found in the cyber security office. [Applicant] stated that he was unaware of any media being in the cyber security office. He stated that everything should have been transferred to [PSO2] when she took over as media custodian. [The] ISSO stated that the Spindles of media were found when the cyber security team were unpacking boxes of supplies for their office after their office went through construction of new furniture around 19th April 2021, which was then found by Security a few days later. [AW1] states that the media was simply overlooked during this unpacking process and must have been from the previous media custodian that was missed during handoff. See Reference A & C [Applicant's MFR dated June 2, 2021 and AE P].

(GE 8 at 3)

During an after-hours inspection on April 21, 2021, security personnel "found one un-opened packet of CD's and one un-opened packet of DVD's in an unlocked cabinet in the Information Assurance office in violation of [SAPCO insider threat implementation guidance dated May 31, 2016]." (GE 7 at 7-8) The media was found in Applicant's office in the SAPF. GW1 testified multiple people could have had access to that office, downloaded critical information and walked out the door undetected. The security concern is that this media had not been brought to the media custodian for accountability as required by SAPCO insider threat guidance whether the media is loose or wrapped. (Tr. 86-91) GW1 testified there is a requirement that "any media that comes into a SAPF has to be accounted for" by the media custodian. (Tr. 145-48) GW3 testified blank media may be referred to as "manufactured." (Tr. 254-55)

The preliminary inquiry also found:

> There were shipments of [encryption devices] brought into the SAPF with manufactured media that [were] not discovered upon initial inspection but instead [on] a later date by security. [Applicant] states the shipment of [encryption devices] were received and brought into the SAPF, where they were briefly inspected. During the brief inspection of the shipment, the CDs went unnoticed. Upon discovery at a later date from security, a different inspection of multiple CDs [was] brought under control by security and determined to be manufactured CDs with the shipment. [Applicant] states even though he was unaware of the manufactured CDs, the JSIG MP-4 states manufactured sealed media is not required to be controlled by the media custodian. No internal SOP exists currently within the SAPF, however an internal "Security Stand Down Training" was conducted around February 11th [2021] for employees within the SAPF, outlining policies. procedures and expectations from all employees. At this training how to handle incoming media was discussed along with handling procedures for all internal media inside the SAPF. See Reference A.

(GE 8 at 3-4, GE 7 at 9-10)

Applicant was not present when encryption devices he ordered were delivered on or about April 28, 2021. (GE 7 at 9-10; Tr. 97-99, 365-67) GW1 reported Applicant provided guidance to put the encryption devices with existing inventory in the SAPF. Security personnel entered the inventory space and found "opened boxes containing [encryption devices and manufacturer media]." (GE 7 at 9) PSO2 and CSS conducted an inventory and "confiscated six CD's that had not been brought to security for accountability." (GE 7 at 9) GW1's report noted Applicant briefed SAPF media control requirements, including incoming media, while training others on media custodian responsibilities on February 23, 2021. (GE 7 at 9-10) GW1 testified Applicant's conduct was "typical of the loose controls that [he] exhibited while he was the media custodian, but then even disregarded the procedure to take all that media to the new media custodian and to security so that they could bring it into accountability." (Tr. 97)

Applicant asserted "Manufactured CD's, whether commercial software maintained by IT personnel or factory-sealed fresh media, are specifically excluded from media control requirements per policy" and cited various references. (SOR Response at 7-8) The JSIG "Exempts new, unused, factory-sealed media from marking as long as the media remains within [organization-defined controlled areas]" and "Factory Fresh Media. Factory-sealed media does not need to be controlled until opened. Once opened, this media must be brought under control and stored within the SAPF in a locked cabinet under the control of the Media Custodian. At no time will any other users be permitted to have free access to blank media" (AE BB at 2, 4-5) The JSIG specifies, the PSO "provides security control measures for [digital media and that] All digital media . . . must be authorized by the PSO . . . prior to being introduced into the SAPF. Organizations are required to ensure the local facility SOP defines personnel/roles and security measures used to control access to media[.]" (AE BB at 2). Applicant was no longer the media

custodian in April 2021 and otherwise testified consistently with his SOR response and the references he provided. (Tr. 365-70, 436-40, 553-57)

PM2 noted the bulk media (presumably the spindles of CDs/DVDs) was in its original wrapping, that as part of ongoing renovations SAPF office contents were boxed up and moved around during that timeframe, that it is possible the boxes were misplaced during the shuffle, and that it is more likely the media had not been given to the recently appointed media custodian during transition. (AE TT at 2) AW1's testimony was consistent with PM2's. (Tr. 591-93)

There is insufficient evidence to determine when the spindles including an un-opened packet of CDs and an un-opened packet of DVDs were introduced into the SAPF or whether Applicant was the media custodian at the time. Although there is substantial evidence the un-opened spindles of media should not have been in an unlocked cabinet in Applicant's SAPF office in April 2021 and that the spindles of media had not been provided to security or to the then-media custodian for accountability, neither of those matters were alleged in the SOR. The most plausible explanation is that the unopened media was introduced into the SAPF while Applicant was media custodian and that it was not transferred to the new media custodian when duties transitioned to security, but that was not alleged in the SOR.

With respect to the manufactured media found with encryption devices, Applicant testified PSO2's statement confirms security personnel introduced the encryption devices into the SAPF. (Tr. 367-68) He was unable to identify a specific reference to support his claim, and my review of the evidence revealed no specific statement from PSO2 that supported his claim. However, record copies of PSO2's statement are heavily redacted. (Tr. 367-69; GE 11; AE L) Applicant submitted evidence encryption devices he ordered were packaged on April 27, 2021, and received on April 29, 2021, by someone other than him. (AE K) He testified these were the encryption devices discussed above. (Tr. 367) He noted security is responsible for inspecting hardware that enters the SAPF. (Tr. 368-69) He anticipated receiving only the encryption devices because they were being shipped from a military distribution center, but acknowledged that security found "a disc, a closed, manufacturer-sealed disc that contained drivers." (Tr. 369, 436-37) He claimed this was not unusual, that "manufactured media is excluded from media control purposes," and that it was not attributable to anything he did. (Tr. 369-70)

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 PSO2 and CSS "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.

SOR ¶ 1.i: In or around January 2021, you failed, as required by your position as designated media custodian, to train multiple employees on the Two Person integrity process before appointing them to data transfer positions. Applicant denied the allegation.

On January 8, 2021, a DTA requested a disc for a data transfer and Applicant responded that his request would have to wait because he was out sick with COVID and was the only appointed media custodian. (AE V) PM2 and PSO2 approved a waiver citing time sensitive mission requirements with the understanding the media would be turned over to Applicant when he returned to work. (GE 4 at 1; Tr. 334-36) On January 28, 2021,

> [Applicant] reported to security that [two DTAs] had not conducted TPI on the ad hoc media loan. After an exhaustive investigation, [the DTA's were found] not culpable of an infraction as [Applicant] did not provide adequate training. [When questioned by PSO2, Applicant stated] the in-depth training was in the draft [SOP which] was in [PM2's] office for review but was never provided to the [DTA's]. The [DTA's] can't be held responsible for guidance not provided to them. . . . After concluding the investigation, [PSO2] determined [Applicant] committed a security infraction by not ensuring DTAs were properly trained before appointing them [as DTAs]. In response, [PSO2] appointed individuals within the security office as Media Custodians, thereby removing [Applicant] as the Media Custodian.

(GE 4 at 1-2)

SAPCO concurred in the information provided in the incident report and mitigating actions taken, categorized the incident as an infraction, and considered it closed. (GE 5)

Applicant asserts "media custodians are not delegated the authority to appoint [DTAs]" and that as media custodian he did not appoint DTAs. His claims the roles are required to have separation-of-duties, that media custodians are not required to train prospective DTAs and that security personnel are required to create and implement a security education training and awareness (SETA) program for assigned programs are corroborated in part by applicable regulations. (SOR Response at 9-10; Tr. 336-39, 466-86; AE X at 6-7; AE AA at 2) Security officials are generally responsible for establishing a SETA program for their SAPs, initial briefings and annual training of SAP-accessed individuals. Annual training by security personnel "or designee may take several different forms . . . or other methods as approved by the PSO." (AE Y at 3; Tr. 336-38, 370)

There is insufficient evidence to find that, as DTA, Applicant was required to train DTAs on the TPI process, was authorized to or appointed DTAs, or to find that he appointed DTAs in or around January 2021.

Applicant and AW1 confirmed that as ISSM's, they appointed the two DTA's for IS they managed after confirming completion of required training. As ISSM, Applicant appointed the DTAs to conduct data transfers on IS2 and AW1 and appointed them to conduct data transfers on IS3. ISSMs use standardized training for "low risk and high risk" transfers provided by higher authority that "does not go into very much depth as far as the TPI process." (Tr. 575-80; AE HH) Applicant said the January 2021 TPI incident occurred on IS3. (Tr. 467-73) GW1 testified Applicant "supported" AW1 in his role as ISSM for IS3. (AE M at 5; GE 7 at 6; Tr. 84, 102, 469-72) Applicant and AW1 stated the transition from IS2 to IS3 occurred in November or December 2020. (Tr. 521, 579, 763-64; AE GG)

Applicant acknowledged the two DTAs requested training before being appointed as DTAs (date and IS not identified), said he pointed them to security, and provided them with a PowerPoint presentation. (Tr. 472-73) Emails from October 2020 show Applicant provided training slides prepared by a service-level special programs office to the then-prospective DTA "for the requisite approval of low risk DTA," and required a response with "a digitally signed and encrypted email stating [she] completed the training[.]" (AE FF, AE HH, AE Q at 3) Applicant did not know how long they had been DTAs on IS3 and stated that prior to this incident the DTAs had complied with TPI requirements. (Tr. 483-85) He did not see GE 4-5 until after receiving the SOR and asserted the PSO is responsible for the SETA program which covers insider threat and DTA responsibilities. (Tr. 336-339, 466-86; AE F at 5; AE X at 6-7)

GW3 testified the draft SOP stated "training would be conducted by the ISSM and the employees both stated that [Applicant] was the one that gave them training." (Tr. 216) GW3 said it would be fine for Applicant to provide training to DTAs "so long as they had it in the processes as they had in their draft form, and they're knowledgeable of what the process should be." (Tr. 215-18) Emails from February 2021 indicate Applicant forwarded a certificate showing that one DTA completed required training and stated he was trying to obtain a certificate for the other. (AE GG-HH)

There is substantial evidence that, as ISSM, Applicant provided training slides to prospective DTAs in about October 2020, appointed DTAs for IS2, and assisted AW1, the ISSM for IS3. There is substantial evidence that Applicant was aware the draft SOP required ISSMs to train prospective DTAs before appointing them as DTAs and that he provided some training to them. It is unclear if the ISSM was required to train prospective DTAs on the TPI process and the SOP had not been approved at the time. Nevertheless, Department Counsel did not move to amend the allegation to comport with the evidence, and the evidence is insufficient to establish the allegation as alleged. ISCR Case No. 12-11375 at 5 (App. Bd. Jun. 17, 2016) (administrative pleadings "should be liberally construed and easily amended. . . . The purpose of an SOR is to give an applicant adequate notice of the allegations . . . so that the applicant has a reasonable opportunity to respond to them") (citation omitted). This allegation is decided for Applicant.

SOR ¶ 1.j: In or around [April] 2021, while designated [ISSM], you improperly allowed multiple packages containing USB drives to enter the facility. When asked

whether you had inspected the packages or were aware of their contents, you stated that, despite being the designated media custodian, it was "not your responsibility to track all media." Over Applicant's objection I provisionally granted Department Counsel's motion to amend the allegation by substituting the words "around [April] 2021, while designated [ISSM]" and deleting the words "March" and "media custodian." (Tr. 87-91)

Applicant denied the allegation explaining he was not the appointed media custodian when the issue allegedly occurred. He did not recall saying it was "not my responsibility to track all media [and explained] that unopened media in its original packaging is not required to be tracked until after it is opened." He stated: (1) the USB drives in question were factory-installed drivers for a television installed in an organization conference room in about April 2021; (2) he was not the primary point of contact and was not notified when the devices were delivered or installed; (3) he received an email from the security manager on April 22, 2021 and responded the next day identifying the televisions contained USB drives and recommended the USB drives be collected and destroyed. (SOR Response at 10-11)

A preliminary inquiry conducted by CSS dated June 30, 2021 found:

> Three USB drives were discovered when a new TV procurement was installed in multiple locations within the SAPF around March 5th. After Installation of the TV's, a (sic) hardware box for each TV was left (3 Total) which was not brought to security's attention until a later date. In each of these boxes consisted of a USB drive and other materials, which was brought under control and brought to the attention of [Applicant] who was the media custodian at that time. [Applicant] stated the TV's were installed without his awareness to be able to track this. When asked if he knew about the contents of the package (to include the USB drives) that would be delivered when he procured them, he replied with it was not his responsibility to track all media. See Reference A [Applicant's Memorandum for the Record dated June 2, 2021].

(GE 8 at 3)

Applicant testified consistently with his SOR response stating he was not media custodian on March 5, 2021, and that PSO2 and another security member brought three televisions into the SAPF he had previously recommended they buy. He said that he was not in the office at the time, that security unpacked the televisions and had a contractor install them. After finding USB drives among the packaging, PSO2 contacted Applicant and asked him, as ISSM, what they should do with the USB drives. He recommended they mark and then destroy the USB drives. He said PM2 likely approved the purchase. (Tr. 369-73; AE X at 11-12) He submitted emails dated April 22 and 23, 2021 with PSO2 addressing three televisions with USB drives including his recommendation to dispose of the USB drives so they did not have to be tracked as removeable media after properly moving the firmware drivers "onto a system." (AE T)

PM2 stated the TVs were under inventory control, but the original boxes had not been opened yet. PM2 approved the original purchase order, said there was no indication a thumb drive would be shipped with the TV, and that there was no way to know what was in the box until it was opened. Once it was opened, which Applicant was not present for, the thumb drive was immediately reported to security. PM2 asserted the correct procedure was followed. (AE TT)

Applicant was not the media custodian when the televisions with USBs were delivered. The TVs were under inventory control when Applicant, as ISSM, confirmed the packages contained USB drives, and provided appropriate disposition guidance and corroborating documentary evidence. This allegation is found for Applicant.

SOR ¶ 1.k: In or around March 2021, you were removed as designated media custodian following one or more security infractions. Applicant denied the allegation and denied receiving notification or corrective guidance "related to any alleged security infraction involving [his] role as media custodian at the time [those] responsibilities were transitioned." (SOR Response at 11)

It appears Applicant was removed as media custodian by the PM because of security concerns raised in February 2021 about him performing duties as both ISSM and as media custodian. There is also evidence he was removed as media custodian because of the security infraction alleged in SOR ¶ 1.i. (Tr. 45-46; GE 4 at 2) Media custodian responsibilities were transferred from Applicant to program security office personnel on or shortly after February 23, 2021. (AE U; GE 6 at 2, GE 7 at 4; Tr. 45-47, 98-99) Although there is substantial evidence supporting the allegation, administrative actions taken as a result of a security infraction do not constitute an independent security concern; it does not allege a potentially disqualifying security concern; and the security infraction alleged in SOR ¶ 1.i. is addressed above. This allegation is found for Applicant.

SOR ¶ 1.l: In or around April 2021, you improperly carried a Bluetooth-enabled wallet, which contained a tracker card, into a secure environment. Applicant admitted this allegation explaining that on February 15, 2021, the day after receiving a "wallet containing a Bluetooth-enabled card for loss prevention", "during a discussion of the wallet features with security personnel, [he] realized that [he] had accidently brought it into [a secured] space . . . immediately self-reported to the cognizant security authority, and immediately removed the device from the space." (SOR Response at 12-13) He claimed this type of infraction "is not uncommon," that his prompt report of his unintentional infraction and removal of the prohibited item were appropriate actions, and that such infractions normally result in remedial training. Applicant acknowledged he was advised that he brought a prohibited device into the SAPF but said he "did not receive remedial counseling." (*Id*. at 13; Tr. 331-35, 790)

A report of the incident dated April 28, 2021, corroborated Applicant's rendition and identified February 17, 2021, as the date of the incident. The report characterized Applicant's actions as an infraction, assessed the risk of compromise as low, and noted he was verbally counseled on the prohibited items policy applicable to SAP. (GE 2) The

service SAPCO concurred in the assessment and mitigating actions taken, and the incident was closed on May 20, 2021. (GE 3; Tr. 333) This allegation is established.

There is no evidence that any of the security incidents alleged in the SOR resulted in the compromise of classified information or otherwise impacted national security. (SOR Response; GE 2-10; AE SS-TT) Preliminary inquiries of matters alleged in SOR ¶¶ 1.i and 1.l. concluded the risk of compromise was low. (GE 2-5) The report of matters alleged in SOR ¶¶ 1.a-1.h, and 1.j concluded the loss or compromise of SAP information cannot be ruled out.

Character Evidence

Five witnesses testified and Applicant submitted numerous letters of recommendation and character references from a general officer, senior government civilian employees, his employer and others including current and former supervisors, colleagues, and friends. The witnesses and letters favorably commented on his integrity, trustworthiness, judgment, reliability, work performance, cybersecurity and special programs expertise, professionalism, handling of classified and sensitive information, mission-focus, solution-oriented approach, and his commitment to national security. Many of the witnesses and letters directly recommend or support approval of his continued access to classified information. (SOR Response; Tr. 557-713; AE A-B, D-H, J, M, U, X, OO, SS-TT) He also received a large retention bonus in 2023. (AE I, AE OO)

PM1, now a general officer, commented favorably on Applicant's character and performance. He rated Applicant "significantly higher than his peers," called him "a self-starter who tackles challenges head on", and a problem-solver. He stated Applicant is not a security risk and would gladly be welcomed back to the team. He hopes to help "clear [Applicant's] name and allow him to get back to helping our [warfighters]." He noted that when Applicant came to the program there were about 30 systems at risk of being shut down because they were significantly behind on testing and paperwork necessary to justify their ATO. Applicant immediately recognized the problem, coordinated with higher headquarters, developed a plan, resolved the problem within six months, and all ATOs were approved. He stated that Applicant corrected problems in the SAPF without assistance from leadership. (AE SS)

Applicant said he requested but did not receive formal training regarding media custodian duties prior to his appointment in March 2020. He acknowledged reviewing relevant policy and procedures and receiving a rough draft SOP from his predecessor that he revised based on issues he experienced as media custodian. He participated in a security training stand-down on February 11, 2021, that covered topics including guidance regarding media custodian duties and said it was the first training he recalled receiving from organization security. Applicant confirmed previously receiving extensive training on rules and regulations associated with the handling of SAP information and SAPFs including annual training and noted he has various accreditations. As ISSM he oversaw training of prospective DTAs and previously served as a DTA. He stated the only remedial counseling received regarding any suspected security incident was when he

was told the Bluetooth-enabled wallet was a prohibited device after he brought it into the SAPF. He denied receiving remedial training after the suspected security incidents but received some security training from his employer after his SAP access was suspended. (SOR Response at 9-10, 13; Tr. 147-51, 333-39, 451-59, 499-500, 733-34, 783-95)

Applicant 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." (Tr. 458) He was "[v]ery familiar" with rules and regulations applicable to media custodian duties and previously served as a DTA with "burn privileges." (Tr. 458-59) He recalled that when SAPCO updated the insider threat guidance and JSIG in 2016 he was provided with "relevant material" and "self-trained" on the updated material. (Tr. 459)

Applicant testified this process has been very humbling and that he never anticipated it would get this far. He acknowledged being very upset about the way the entire matter was handled and expressed regrets for not handling it differently. He stated he has continued efforts to be professional with everyone he works with including security personnel and expressed his openness to remedial training to address any deficiencies. He said there was a draft SOP at the time and that he provided input on both ISSM and media custodian duties. I noted the record did not include statements from PM1 or PM2, and post-hearing, Applicant submitted statements from both. (Tr. 782-90; AE SS-TT)

Applicant testified any incidents were inadvertent or unintentional and that most were due to interpretation of policies and regulations in the absence of an SOP. He noted his immediate reporting of the DTA TPI incident and of his improper introduction of a Bluetooth-enabled wallet into a secure environment. In his 18 years as a cleared federal contractor and cybersecurity professional his primary roles have been to ensure the protection of IS through the implementation and validation of security controls and he has received favorable recognition for his performance ensuring the protection of classified and sensitive government information. He had no security incidents prior to or since those alleged in the SOR. (Tr. 787-89; SOR Response)

Matters Not Alleged in the SOR

In his November 2021 SCA, Applicant reported a memo was provided to his employer stating that "3 security reports (2 infractions and 1 violation)" had been filed by PSO2 and that "they have removed [his] physical access to a classified area[.]" (GE 1 at 15) In response to another question in the SCA he denied that he "**EVER** had a security clearance eligibility/authorization denied, suspended or revoked." (GE 1 at 44) The following colloquy occurred during cross-examination regarding his incorrect answer.

> [Applicant] I probably failed to understand that question because I did not, like I thought it was saying, have you ever like before. Like I did not understand why I was filling that out again. . . . I was not like trying to speak incorrectly there. I knew that I had allegations. And I knew that [SAPCO

> notified me it was suspended] which is stated in there. But I didn't, I didn't know that it was adjudicated yet. That's where my, where my confusion was.
>
> [Department Counsel] So, you were confused by the phrase, have you ever had a security clearance eligibility/access authorized, denied, suspended, or revoked. You read that to mean that it had to be fully adjudicated?
>
> [Applicant] I thought, yes, ma'am, I thought that it, I thought we were in the middle of this discussion and incident, investigation as it were, right, and that it needed to be adjudicated before – that's all I was requesting this whole time is everything was moving so fast and I just wanted to like understand what the allegations were and talk about it because I'd never been in a situation like this before. So, I was trying to understand like hey, like is this adjudicated? Should I answer like this? And [the FSOs] gave me an opportunity to clarify, rectify it and I did that . . . .
>
> [Applicant] I completed it based on my judgment. When [the FSOs] got it they said, hey, this is not accurate. And I said, okay. Like please explain why. My concern is it was going to go on my record. I do not want, I did not want anything like that on my record especially when I thought we were still trying to adjudicate it. So, yes, I answered as truthfully as I thought was where we were at in the process. And then I asked [my FSO] to support me in the process, which she did not. . . . After the fact [the FSO told me] that I needed to fix it which I did.

(Tr. 500-502)

Applicant subsequently submitted an email addressing his perception of the above testimony and summarizing an exhibit consisting of emails addressing his request to revise his November 2021 SCA. (AE QQ at 4, AE MM) He provided a different explanation for his failure to disclose his SAP access had been suspended in his SCA:

> I believe the Department Coun[sel] was asserting that I lied on my security clearance application because this would've taken place after I was removed from the SAP space. I'll admit that I was shaken by this allegation, and testified that I did recall having a conversation with my FSO . . . about it, and definitely did not intend to lie on the application. At the time I believed that the question was asking about suspension of my actual clearance, not my SAP access. After going back through my records I located this email chain where I did in fact immediately request that it be updated to show that I had been suspended from a space.

(AE QQ at 4)

Applicant submitted an email to his employer's security associate stating he needed to revise his SCA to state his SAP access had been suspended and the security

associate's response that his SCA could be returned to him if necessary. His email is dated the same day and time stamped within an hour of the time stamp on his certified SCA, but it is unclear if the email was submitted before or after he certified the SCA because of potential time zone differences. Applicant submitted no documentary evidence he corrected his response to the SCA suspension question or that he certified and submitted a revised SCA. (AE MM; GE 1 at 15, 44, GE 10; Tr. 495-504, 784-86)

Policies

"[N]o one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). As Commander in Chief, the President has the authority to "control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to have access to such information." *Id.* at 527. The President has authorized the Secretary of Defense or his designee to grant applicants eligibility for access to classified information "only upon a finding that it is clearly consistent with the national interest to do so." Exec. Or. 10865 § 2.

Eligibility for a security clearance is predicated upon the applicant meeting the criteria contained in the adjudicative guidelines. These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, an administrative judge applies these guidelines in conjunction with an evaluation of the whole person. An administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. An administrative judge must consider all available and reliable information about the person, past and present, favorable and unfavorable.

The Government reposes a high degree of trust and confidence in persons with access to classified information. This relationship transcends normal duty hours and endures throughout off-duty hours. Decisions include, by necessity, consideration of the possible risk that the applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation about potential, rather than actual, risk of compromise of classified information.

Clearance decisions must be made "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." Exec. Or. 10865 § 7. Thus, a decision to deny a security clearance is merely an indication the applicant has not met the strict guidelines the President and the Secretary of Defense have established for issuing a clearance.

Initially, the Government must establish, by substantial evidence, conditions in the personal or professional history of the applicant that may disqualify the applicant from being eligible for access to classified information. The Government has the burden of establishing controverted facts alleged in the SOR. *See Egan*, 484 U.S. at 531. "Substantial evidence" is "more than a scintilla but less than a preponderance." *See v. Washington Metro. Area Transit Auth.*, 36 F.3d 375, 380 (4th Cir. 1994); *see also* ISCR Case No. 18-00496 at 3 (App. Bd. Nov. 8, 2019) (citations omitted). The guidelines

presume a nexus or rational connection between proven conduct under any of the criteria listed therein and an applicant's security suitability. *See* ISCR Case No. 15-01253 at 3 (App. Bd. Apr. 20, 2016).

Once the Government establishes a disqualifying condition by substantial evidence, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. Directive ¶ E3.1.15. An applicant has the burden of proving a mitigating condition, and the burden of disproving it never shifts to the Government. *See* ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005).

An applicant "has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his security clearance." ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002). "[S]ecurity clearance determinations should err, if they must, on the side of denials." *Egan*, 484 U.S. at 531.

Analysis

Guideline K (Handling Protected Information)

The concern under this guideline is set out in AG ¶ 33:

> Deliberate or negligent failure to comply with rules and regulations for handling protected information--which includes classified and other sensitive government information, and proprietary information--raises doubt about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern.

Neither a violation of a specific rule nor an actual loss of classified or sensitive information is required to establish a Guideline K concern if the conduct has security significance. ISCR Case No. 11-05079 at 5-6 (App. Bd. Jun. 6, 2012). "Security significant conduct may be ascertained through the application of common sense with reference to the broad, overall goal of protecting such information." *Id*. at 5 (citing ISCR Case No. 07-00852 at 4 (App. Bd. May 27, 2008)) (In analyzing cases before them, Judges must be guided by common sense and with a view toward making a reasoned determination consistent with the interests of national security).

As discussed above, I found that Applicant refuted the allegations in SOR ¶¶ 1.a, 1.c, 1.i, 1.j, and 1.k.

AG ¶ 34 provides conditions that could raise a security concern and may be disqualifying. The following are potentially applicable:

> (g) any failure to comply with rules for the protection of classified or sensitive information;

(h) negligence or lax security practices that persist despite counseling by management; and

(i) failure to comply with rules or regulations that results in damage to the national security, regardless of whether it was deliberate or negligent.

The preliminary inquiries, witness testimony and other documentary evidence provide substantial evidence that Applicant: improperly issued bulk media for future use including for convenience or for no specific purpose (SOR ¶ 1.b); failed to properly control and account for media used or intended for use with SAP information (SOR ¶¶ 1.d-1.f, 1.h), and that he improperly allowed manufactured CD's to be introduced into a controlled space (SOR ¶ 1.g). Applicant admitted improperly introducing a Bluetooth-enabled device into a secure environment (SOR ¶ 1.l). I also find the conduct has security significance. *See* ISCR Case No. 11-05079 at 5-6 (App. Bd. Jun. 6, 2012). AG ¶ 34(g) is established for the conduct alleged in SOR ¶¶ 1.b, 1.d-1.h and 1.l.

AG ¶ 34(h) is not established for conduct alleged in SOR ¶¶ 1.b, 1.d-1.f, 1.h, and 1.l because the conduct occurred before Applicant improperly introduced a Bluetooth-enabled device into a secure environment and before he was counseled for doing so.

AG ¶ 34(h) is not fully established for the conduct alleged in SOR ¶ 1.g. There is insufficient evidence to determine if any of the CDs confiscated by security were introduced into a controlled space after Applicant was verbally counseled on the prohibited items policy applicable to SAP (*See* SOR ¶ 1.l).

AG ¶ 34(i) is not established. Although a report to SAPCO assessed the loss or compromise of SAP information could not be ruled out, there is no evidence conduct alleged in SOR ¶¶ 1.b, 1.d-1.h or 1.l resulted in damage to the national security.

Additional discussion of the established disqualifying condition is in the mitigation section, *infra*. Conditions that could potentially mitigate security concerns under AG ¶ 35 include:

(a) so much time has elapsed since the behavior, or it has happened so infrequently or under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;

(b) the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities;

(c) the security violations were due to improper or inadequate training or unclear instructions; and

(d) the violation was inadvertent, it was promptly reported, there is no evidence of compromise, and it does not suggest a pattern.

Security violations "strike at the heart of the industrial security program" and are one of the strongest possible reasons for denying or revoking access to classified information, because they raise serious questions about an applicant's suitability for access to classified information. ISCR Case No. 03-26888 at 1 (App. Bd. Oct. 5, 2006). Once it is shown that an applicant has committed such violations, he or she has a "very heavy burden" in demonstrating mitigation. ISCR Case No. 14-05127 at 8 (App. Bd. June 24, 2016).

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.

Applicant did not conduct a full audit of media in the SAPF when he assumed duties as media custodian. I find his claims that his attempts to do so were inhibited because of security concerns (PSO1 and later PSO2) expressed over granting him access to certain information in some safes and at least one room to be credible and corroborated in part by AW1. His claims that he elevated requests for access to the denied areas to PM2 are corroborated in part by AW1, but PM2's post-hearing statement does not address safe or room access.

Applicant's 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 that he believed he had seen a media log in "spreadsheet format, very similar to the template" prescribed by SAPCO. However, record evidence raises questions as to whether Applicant maintained a chronological and serial log in accordance with the sample media log template as required by SAPCO. He did not use the "Media Control Number" or "Type of Media" conventions specified in the sample log. The DTQs in evidence show Applicant issued eight pieces of media with four nearly identical control numbers, that the media was not issued sequentially, and that two of the DTQs included significant discrepancies (one failed to identify where data was transferred to (i.e. purpose), and another failed to identify the date and time of media disposition). Although Applicant reported that AW1 and his team were trying to obtain copies of additional DTQs scanned to a secure IS and to obtain approval to export those DTQs, he did not submit additional DTQs or request additional time to do so.

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. Although AW1 initially testified there were media logs for media issued from August 2020 to February 2021, he clarified that he had not seen a media log or spreadsheet after the August 2020 hard drive failure and had seen only scanned copies of DTQs uploaded by Applicant from August 2020 to February 2021. Additionally, Applicant's claim the December hard drive failure occurred while a colleague was imaging his computer's hard drive while attempting to migrate data to IS3 is unsupported by other evidence. Applicant did not submit a statement from the colleague he said was imaging the hard drive when it failed, after saying "I can get that to you". (Tr. 757-58)

Applicant's claims that 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 personnel are untrue. His belated admission that he provided security personnel with scanned copies of DTQs for media distributed from August 2020 to February 2021 and not a spreadsheet consistent with SAPCO requirements is corroborated and established as fact.

Applicant's claim that a DTQ includes essentially the same information as a media log and could be used to recreate a media log that satisfies SAPCO requirements is corroborated in part and refuted in part. A DTQ may be used to substantially re-create a media log because it includes much but not all data required to be entered into a media log by the media custodian. A DTQ includes derivative documentation prepared by a DTA, not the media custodian, and the DTQs in evidence do not show the number of logs, the number of media entered control or when the media was entered in control and does not include sufficient information to determine if there was an insider threat problem. In his SOR response, Applicant acknowledged he could not regenerate logs for several pieces of media from the DTQs and two of the eight DTQs in the record include significant discrepancies (one failed to identify where data was transferred to and another failed to identify the date/time of media disposition).

Applicant has categorically denied the allegations in SOR ¶¶ 1.b, and 1.d-1.h. Given the absence of media logs, contradictory evidence and testimony and claims that he was unfairly targeted by security personnel, his testimony and credibility are particularly significant in determining whether he carried his burden to mitigate security concerns. After review of the entire record, I have significant concerns about Applicant's credibility and judgment for the following reasons:

First, Applicant's testimony 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 is untrue. Applicant confirmed the falsity of this testimony on the third day of the hearing when he admitted he had not provided security a media log (which he claimed to maintain in an Excel spreadsheet) but had instead provided security personnel scanned copies of DTQs.

Second, Applicant's explanations for why he claimed to turn over media logs to security personnel and that security personnel lied about not receiving them were not credible for the following reasons:

(1) he lied about turning over "a digital Excel spreadsheet" media log;

(2) his claim that he thought the SOR allegation meant he had not given security personnel anything is contradicted by the plain language of the allegation (he failed to properly maintain media logs as required);

(3) discrepancies between his SOR Response, statements and testimony including: (a) whether a hard drive failure occurred on December 21, 2020 or in January 2021, (b) whether the hard drive failure occurred before or while he was out sick with COVID, and (c) discrepancies in his testimony that after returning to office following his bout with COVID (late January or February 2021) he "tried to fill out the media custodial log to show TPI accountability", and his testimony the media log was lost in December 2020 and that he had not tried to recreate it before media custodian duties were transferred in February 2021, and

(4) his persistent efforts to equate a DTQ to a media log and to cast aspersions on security personnel based upon his opinion the two documents were essentially the same until the third and final day of the hearing suggest an intent to deceive and/or raise significant questions about his judgment. Applicant acknowledged he was unable to regenerate logs for several pieces of media in his SOR Response. He also acknowledged that he did not know exactly how many pieces of media he distributed while serving as media custodian but estimated the number at "60 or so". He also claimed, without corroboration, that AW1 and his team reviewed available records and believed the number to be "consistent with what [Applicant] believed to be, like 60 or so."

Third, I found his testimony and demeanor at the hearing to be unconvincing and inconsistent with someone who was reliably telling the truth.

Fourth, matters not alleged in the SOR raise additional credibility and judgment concerns. Although unalleged conduct may not be considered for disqualifying purposes, it may be considered to: (a) assess Applicant's credibility; (b) evaluate his evidence of extenuation, mitigation, or changed circumstances; (c) consider whether he has demonstrated successful rehabilitation; (d) decide whether a particular provision of the Adjudicative Guidelines is applicable; or (e) for whole-person analysis. *See* ISCR Case No. 03-20327 at 4 (App. Bd. Oct. 26, 2006) I have considered that:

(1) Applicant provided different explanations for failing to disclose his SAP access had been suspended in his November 2021 SCA. He testified that he knew his SAP access was suspended and did not want a suspension on his record before final adjudication but subsequently claimed that he thought the question was about suspension of his security clearance and not his SAP access;

(2) Applicant's claims that he corrected his SCA to show his SAP access was suspended after being informed his November 2021 SCA was incorrect is unsupported by other evidence. There is no evidence he corrected his answer or submitted a revised SCA after his November 2021 SCA (GE 1);

(3) Applicant's unsolicited testimony that he would not have received glowing praise from PM1 and PM2 for his work on the change request and ATO for IS2 if he had not submitted "the appropriate documentation" is disputed by PM2's account that he counseled Applicant because Applicant failed to timely submit the final ATO paperwork and that Applicant admitted the paperwork fell "through the cracks[:]" and

(4) that more than two months after media custodian duties were transferred from Applicant to security, two unopened spindles of blank media, that he was not then authorized to possess, were found in an unlocked cabinet in his office in the SAPF. The most plausible explanation is that the unopened media was introduced into the SAPF while Applicant was media custodian and that he failed to ensure that it was transferred to the newly appointed media custodian.

Fifth, Applicant's actions and words show that he either would not acknowledge or failed to understand the SAP community's greatest insider threat security risk is information system users "with privileged status" like ISSMs. (AE AA at 2) Although he did not volunteer for or apparently desire to perform additional duties as media custodian, his apparent lack of awareness of this fundamental tenet of SAPCO's insider threat guidance and actions he took as media custodian based upon his judgment or interpretation of some rules were inconsistent with a risk-based approach to his duties and raises additional questions about his judgment. To be clear, Applicant was not responsible for his simultaneous appointments as ISSM and media custodian, but he was responsible for his actions. This is particularly true with respect to the clearly enumerated duties of a media custodian to maintain a media log in accordance with the sample provided by SAPCO.

Additionally, AW1's SAP experience, knowledge of most allegations, and personal and professional relationship with Applicant made him an important witness, but parts of his testimony were not credible. He misleadingly testified there were media logs on IS3 for the period August 2020 to February 2021 and then acknowledged he had not seen a media log or spreadsheet during that timeframe. Next, his assertions that media custodians are not required to use the "Sample TPI Media Log", that DTQs are essentially equivalent to a media log and "meet the intent of the [SAPCO insider threat guidance]" are contradicted by the directive's plain language that media custodians "shall maintain a removeable media log IAW the sample template." Likewise, DTQs do not show the number of logs, the number of media entered into control or when the media entered in control and include insufficient information to determine if there is an insider threat problem. These credibility concerns diminished the weight given his testimony.

AG ¶¶ 35(a) and 35(d) are established for the behavior alleged in SOR ¶ 1.l. Applicant accidentally carried a Bluetooth-enabled wallet into a SAPF, promptly reported

it and immediately took responsibility for his error. It occurred long ago, does not suggest a pattern, and there is no evidence of compromise. The behavior is unlikely to recur and does not cast doubt on Applicant's current reliability, trustworthiness, or judgment.

AG ¶ 35(a) is not fully established for the conduct alleged in SOR ¶¶ 1.b and 1.d-1.h. The conduct occurred over a period of less than a year, five or more years ago, and occurred while COVID-19 protocols were in effect. However, Applicant has continued to deny responsibility for conduct alleged in SOR ¶¶ 1.b and 1.d-1.g, and he has not accepted full responsibility for the conduct alleged in SOR ¶ 1.h.

After repeatedly claiming he provided security with media logs when media custodian duties were transitioned and that security personnel were lying when they said he had not, on the third day of the hearing he acknowledged he had not provided security with a media log (SOR ¶ 1.h). He admitted providing security scanned copies of DTQs that he considered almost equal to a media log because they included most information necessary to recreate a media log. He then qualified his accusations that security was lying by stating "I understand security's point that they're saying they didn't [receive a media log]. . . . If they're trying to say they didn't receive logs, my interpretation, understanding of that accusation was we didn't give them. Because they . . . said that to us. They said we gave them nothing." His qualified acknowledgements fall well short of an acceptance of responsibility.

Applicant's failure to accept responsibility for his conduct undercuts a determination that he has reformed and rehabilitated himself. *See* ISCR Case No. 96-0360 at 3-4 (App. Bd. Sep. 25, 1997). 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.

AG ¶ 35(b) is not fully established. On about February 11, 2021, Applicant participated in training outlining policies. procedures and expectations for those working in the SAPF including guidance on media custodian duties. On or after February 17, 2021, he was reminded of the prohibited items policy after carrying a Bluetooth-enabled wallet into a SAPF that PSO2 characterized as counseling. After his SAP access was suspended in August 2021, he received some security training from his employer. However, Applicant denied receiving remedial training and denied receiving counseling, except for being told the Bluetooth-enabled wallet was a prohibited device when he carried it into the SAPF. Although he has expressed willingness to participate in remedial training, his denials of security concerning conduct, claims that policy differences were the source of many of the allegations and his propensity to blame others for errors within

his cognizance detract from a conclusion that he responded favorably to counseling and now demonstrates a positive attitude towards the discharge of security responsibilities.

AG ¶ 35(c) is not fully established. Applicant's assertions that this lack of training (notwithstanding his requests) contributed to varying policy interpretations are corroborated in part by the record. There is no evidence he received formal training before his appointment as media custodian. However, he has extensive SAP and SAPF experience, training and certifications. He has been an ISSM and a DTA, and testified his past close working relationship with media custodians made him "[v]ery familiar" with applicable rules and regulations. He "understood all their process, their policies, and their execution of their job functions" and "self-trained" on updated insider threat guidance and the JSIG in 2016. His 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. (Tr. 458-59)

AG ¶ 35(d) is not established for the security concerns alleged in SOR ¶¶ 1.b and 1.d-1.h.

Whole-Person Concept

Under AG ¶ 2(c), the ultimate determination of whether to grant eligibility for a security clearance must be an overall commonsense judgment based upon careful consideration of the guidelines and the whole-person concept. In applying the whole-person concept, an administrative judge must evaluate an applicant's eligibility for a security clearance by considering the totality of the applicant's conduct and all relevant circumstances. An administrative judge should consider the nine adjudicative process factors listed at AG ¶ 2(d):

> (1) the nature, extent, and seriousness of the conduct; (2) the circumstances surrounding the conduct, to include knowledgeable participation; (3) the frequency and recency of the conduct; (4) the individual's age and maturity at the time of the conduct; (5) the extent to which participation is voluntary; (6) the presence or absence of rehabilitation and other permanent behavioral changes; (7) the motivation for the conduct; (8) the potential for pressure, coercion, exploitation, or duress; and (9) the likelihood of continuation or recurrence.

I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case. I have incorporated my comments under Guideline K in my whole-person analysis. Some of the factors in AG ¶ 2(d) were already addressed, but some warrant additional comment.

I considered Applicant's age, education, professional certifications, employment record, security clearance history, strong character evidence, reputation as a

cybersecurity professional, and that there is no evidence of other security incidents except those alleged in the SOR or discussed in this decision.

I also considered Applicant has received regular training on information security and the proper handling of classified information including SAP information. I considered that he has worked on significant defense projects, has an excellent reputation for reliability, good character, recognized technical skills, and has a sound record of performance. I also considered that, although the compromise of classified information has not been ruled out, there is no evidence that classified or protected information was compromised.

I considered that he did not receive media custodian-specific training prior to his appointment as media custodian. I also considered that he was unable to complete a full audit of media in the SAPF after assuming media custodian duties because of security concerns expressed by PSO1 and PSO2 and that this inhibited his ability to account for all media in the SAPF. I considered these inhibitions in assessing evidence of Applicant's responsibility for matters alleged in the SOR and focused primarily on his conduct and judgment.

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.

It is well settled that "[o]nce a concern arises regarding an applicant's security clearance eligibility, there is a strong presumption against the grant or maintenance of a security clearance." ISCR Case No. 09-01652 at 3 (App. Bd. Aug. 8, 2011), *citing Dorfmont v. Brown,* 913 F.2d 1399, 1401 (9th Cir. 1990), *cert. denied*, 499 U.S. 905 (1991). Applicant has not overcome that presumption.

After weighing the disqualifying and mitigating conditions under Guideline K and evaluating all the evidence in the context of the whole person, I conclude Applicant has not mitigated handling protected information security concerns. Overall, the record evidence leaves me with questions and doubts as to his eligibility and suitability for a security clearance.

To be clear, Applicant's failure to properly maintain a TPI media log in accordance with SAPCO insider threat guidance (SOR ¶ 1.h) is the most security significant conduct

in this case. Assuming action by higher authority on any or all other finding(s) except SOR ¶ 1.h, I would still conclude, for the reasons discussed above, that Applicant has not met his "very heavy burden" in demonstrating mitigation.

Accordingly, I conclude Applicant has not carried his burden of showing that it is clearly consistent with the national interest to grant him eligibility for access to classified information.

Formal Findings

I make the following formal findings on the allegations in the SOR:

Paragraph 1, Guideline K:	AGAINST APPLICANT
Subparagraph 1.a:	For Applicant
Subparagraph 1.b:	Against Applicant
Subparagraph 1.c:	For Applicant
Subparagraphs 1.d-1.h:	Against Applicant
Subparagraphs 1.i-1.l:	For Applicant

Conclusion

I conclude that it is not clearly consistent with the national security interests of the United States to continue Applicant's eligibility for access to classified information. Clearance is denied.

Eric C. Price
Administrative Judge