In the matter of:	)	
	)	
	)	ISCR Case No. 25-00951
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Karen Moreno-Sayles, Esq., Department Counsel
For Applicant: Elisabeth Baker-Pham, Esq.

09/04/2026

Decision

OLMOS, Bryan J., Administrative Judge:

Applicant mitigated the security concerns raised under Guideline K (Handling Protected Information). Eligibility for access to classified information is granted.

Statement of the Case

On August 13, 2025, the Defense Counterintelligence and Security Agency (DCSA) issued a Statement of Reasons (SOR) to Applicant detailing security concerns under Guideline K. The DCSA issued the SOR 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 Security Executive Agent Directive 4 (SEAD 4), *National Security Adjudicative Guidelines* (AG), effective June 8, 2017.

On January 12, 2026, Applicant answered the SOR (Answer) and requested a hearing before an administrative judge from the Defense Office of Hearings and Appeals (DOHA). The hearing was convened as scheduled on July 16, 2026. Department Counsel offered into evidence Government Exhibits (GX) 1-4, and Applicant offered into evidence Applicant Exhibits (AX) A-C. All exhibits were admitted without objection. Applicant and two witnesses testified. The record closed at the conclusion of the hearing. DOHA received the hearing transcript (Tr.) on July 23, 2026.

Amendment to the SOR

At the beginning of the hearing, Department Counsel amended the SOR, revising subparagraph 1.a to state as follows:

> 1.a. You emailed a file containing protected information you had improperly marked unclassified in about July 2024, while employed with [Company A] in [City, State], that compromised information.

The amendment to the SOR was accepted without objection. (Tr. 11-12)

Findings of Fact

As amended, the SOR alleges that Applicant failed to secure a classified area while employed with Company A on five occasions: in October 2015 (SOR ¶ 1.i), December 2015 (SOR ¶ 1.h), December 2016 (SOR ¶ 1.g), July 2018 (SOR ¶ 1.f), and January 2019 (SOR ¶ 1.e). The SOR further alleges that, in April 2019, she inadvertently provided a folder containing information about a Special Access Program (SAP) to an individual who was not cleared to receive that information (SOR ¶ 1.d). Additionally, the SOR alleges that, once in May 2019 and once in June 2019, she failed to properly secure folders containing classified information (SOR ¶¶ 1.c and 1.b, respectively). Lastly, the SOR alleges that, in July 2024, she improperly marked a document containing classified information as unclassified and emailed it to a colleague on an unclassified network (SOR ¶ 1.a).

With clarifications, Applicant admitted SOR ¶¶ 1.a-1.d and 1.i. She neither admitted nor denied SOR ¶¶ 1.f-1.h and stated she had no direct recollection of the events. I construe her answers to SOR ¶¶ 1.f-1.h as denials. She provided extenuating and mitigating information. Her admissions are incorporated into my findings of fact. After reviewing the pleadings, evidence submitted, and testimony, I make the following additional findings of fact.

Applicant is 42 years old and has one young child. She attended community college from 2004 through 2006. In 2010, she began taking online courses part time and completed a bachelor's degree in 2016. (Answer; GX 1-3; Tr. 31-48, 77)

In 2008, Applicant began working as a subcontractor for Company A, a large government contractor and her current employer. She digitized personnel records and assisted in administrative duties. In 2009, she was offered a full-time contract position as an administrator. She excelled in this position. In 2011, as part of a company reorganization, she began directly supporting the security department of Company A. Later that year, Applicant received her first security clearance. In 2012, while she remained a contractor, she was promoted to work in Company A's visitor center, where she verified individual credentials for access to various company sites that contained classified information. (Answer; GX 1-3; Tr. 34-36)

In 2013, while still working as a Company A subcontractor, Applicant was promoted to badge officer and began working daily tasks within the security department. She created badges, helped a locksmith sign out keys and supported security compliance inspections. In April 2014, she was hired to work for Company A directly as a security representative performing similar duties. (Answer; GX 1-3; Tr. 34-38)

In April 2015, based on her high performance, Applicant began working in the operating center for SAPs. In this position, she supported SAP security officers, generated program access requests, processed personnel security questionnaires, monitored foreign travel and reported any adverse information on employees to government clients. She received a top-secret clearance to support this position. (Answer; GX 1-3; Tr. 36-40)

Applicant testified she received little formal training for her position in the operating center and learned mostly from her own experience in navigating various daily requests. She had access to various SAP names and verified that Company A employees involved with those programs maintained appropriate security credentials and completed annual training requirements. She was also responsible for assisting with physical security including the opening and closing of classified spaces. During an average workday, she navigated over a hundred tasks involving the management and protection of sensitive and classified information. (Answer; Tr. 36-40; 106-108)

One evening in October 2015, Applicant needed to close the SAP operating center for the first time on her own at the end of her shift. This required setting the alarm, spinning the lock and verifying that the digital access code was operational. She believed that she had properly secured the space. However, the next day she learned that the alarm had failed to engage. Company A investigated the incident and categorized the event as a security infraction (SOR ¶ 1.i). She submitted a corroborating statement and was noted in the investigation for being "very cognizant of the security requirements." Applicant testified that she remembered this event because it was her first security infraction. Afterwards, when closing a secure location, she focused on listening for the "beeps" to confirm that the alarm was activated. She still mentions this episode when training new employees. (GX 3-4; Tr. 41-44, 96-98)

Company A records reflect that, in December 2015, Applicant committed another security infraction by failing to fully spin the lock of a secured area containing classified information (SOR ¶ 1.h). Applicant explained that this was considered a "failure to spin" and was categorized as a security infraction as the lock had not engaged. Still, the area was alarmed and required a digital code for entry. She had no direct recollection of this event but did not dispute the summary within Company A's report. (GX 4; Tr. 45-47)

Despite these two incidents, Applicant became the senior member of the SAP operating center in 2016. In this position, she trained new employees and worked to improve various processes for the daily tasks her office received. During this time, she supervised the conversion of over a hundred Company A SAP facilities to updated locking

mechanisms. She also created various matrices for classified meetings that involved multiple SAPs. Later that year, she completed her college degree. (Answer; GX 1-3; Tr. 48-50)

Applicant continued to manage day-to-day operations relating to SAPs including overseeing physical access control, digital compliance and personnel clearance verification. Company A records reflect that, in December 2016, she experienced another security infraction when she "failed to spin" and properly close a classified space (SOR ¶ 1.g). At her hearing, she had no direct recollection of the event but did not dispute the findings within Company A's report. She noted that her workload began to increase during this time, and she often felt overburdened while trying to process multiple tasks at once. She voiced these concerns to management and was told "help was coming." (Answer; GX 4; Tr. 49-52)

In 2017, Applicant accepted a promotion and became a Contractor Special Access Program Security Officer (CSSO). This allowed her to move out of the SAP operating center and directly manage a smaller group of SAPs. However, she discovered that she could not entirely leave her former duties behind. Her replacement in the SAP operating center struggled handling the volume of requests and Applicant felt obliged to assist when possible. (Tr. 50-54)

Applicant was also asked to revamp the annual mandatory training for Company A's various SAPs. At the time, there were over a hundred programs at Company A, and some employees were required to attend upwards of 65 separate 30-minute meetings to satisfy training requirements. Over a three-month period, Applicant assisted in centralizing training where permissible and enabled employees to receive specific packets of information related to their assigned SAPs while limiting the required number of general meetings. (Tr. 50-54)

In 2018, Applicant received another promotion. She was also placed on a committee within Company A where she met with other company security personnel and reviewed any security infractions or violations to determine what mitigating and reporting actions needed to occur. (Answer; Tr. 52-55)

Applicant testified that, during this time, she felt she was doing the work of three people. She consistently worked 12-hour days and answered unclassified emails at home. Additionally, she still maintained her obligations as a CSSO. In July 2018, she received another security infraction for "failure to spin" and properly close a secure area (SOR ¶ 1.f). She raised workload concerns with her management and was again told that "help was coming." That year, she trained five people who were supposed to relieve her of some of her obligations. However, none of them stayed in a position that could provide her assistance. (Answer; Tr. 53-57)

In January 2019, Applicant was promoted to SAP operating center lead. It was intended that she be relieved of her CSSO obligations and be a mentor to new employees.

However, staffing shortages remained and she again struggled to remove herself from various tasks related to the CSSO position. Many employees considered her a subject matter expert in everything security related and "everybody knew who I was. I was regularly stopped for questions, not just to my programs, but to theirs." She stated that as a result, "I couldn't walk across the hall to use the bathroom without it taking ten minutes to get there." She admitted it was not a manageable workload and again raised concerns with management. Again, she was told "help is coming." (Tr. 60-64)

Applicant received four security infractions in 2019. The first occurred in January 2019 when a colleague stopped her in the hallway seeking assistance with securing a classified area as the spin lock was jammed. Applicant attempted to call for assistance but was unable to get through to the SAP operating center. She walked down the hall and tried to place the call again but was interrupted by another colleague regarding an unrelated matter. By the time she completed the second task, she forgot about the first one and concluded her shift with the classified area remaining unsecured (SOR ¶ 1.e). She later learned that a safety pin had not been reset in the door, which caused the spin lock to jam. She testified that she still discusses this incident while training other employees. (Answer; GX 1-4; AX B-C; Tr. 60-64)

In April 2019, during one of Company A's annual SAP training sessions, a colleague asked Applicant to provide temporary support in processing check-ins and handing out relevant SAP materials. Due to a misheard name, Applicant inadvertently transferred SAP materials to an individual not cleared into that specific SAP. He reviewed the information before turning in the folder. Company A noted that this was an "unfortunate" and "unintentional" incident and that there were cover sheets in place that should have alerted the individual that the underlying information was outside of the SAP program he had been authorized to access. Nonetheless, it was considered a security infraction against Applicant (SOR ¶ 1.d). (Answer; GX 1-4; AX B-C; Tr. 65-67)

In discussing this event with her supervisors, Applicant recalled being told to "slow down" in managing her workload. However, she considered her workload to remain at high levels, and she was barely "treading water." This incident caused Company A to rework how it manages handouts of sensitive materials during large training sessions. Applicant assisted in this process. During training sessions, the individual now states their name and employee identification number, and it is read back and confirmed before material is handed over. (Tr. 67-70)

In May 2019, Applicant experienced another security incident when she left a folder containing classified information unattended at her desk. She explained that it was permissible to use the folders to carry classified information, and she used them nearly all day, every day in carrying out her work duties. In this instance, when she shut her office down for the day, she forgot that she left one folder on top of her safe. Following discovery of the folder by another employee, the event was categorized as a security infraction (SOR ¶ 1.c). (Answer; GX 1-2, 4; Tr. 67-69, 114-115)

After this third incident in 2019, Applicant's supervisors met with her to discuss the events and determine what changes needed to occur. At this meeting, Applicant admitted that, while she believed in the mission of the company, she "hated coming into work" and was completely "overwhelmed." She became emotional during the meeting and stated she was exhausted trying to perform multiple jobs for Company A while never receiving promised support. (Tr. 67-70)

While Applicant's management considered options to assist her, in June 2019, she experienced another security incident. While working multiple tasks, she placed two folders carrying classified information in her overhead workspace and forgot to secure them at the end of the workday. They were discovered by another employee during a closing inspection of the workspace. This was determined to be a security infraction (SOR ¶ 1.b). Following this incident, Applicant changed the way she handled the folders and kept the material in her immediate possession as opposed to placing them down in her office. (Answer; GX 1-2, 4; Tr. 68-72, 114-116)

After this last incident in 2019, Company A took action to assist Applicant. She was relieved of her CSSO duties and was permitted to focus her efforts on managing the SAP operations center. She later learned that three new hires were assigned to fill her various CSSO duties. (Tr. 70-73, 112-115)

After the change in her work assignments, Applicant continued to excel with Company A. In 2020, she began working under Mr. V as a CSSO managing various SAPs that involved multiple worksites. One of her first duties involved coordinating with engineers and assisting with the opening of a new laboratory. She also drafted standard operating procedures (SOPs) for the laboratory to remain compliant with government security requirements. (Tr. 75-76, 112-114, 119-120)

In 2021, while pregnant, Applicant traveled cross-country to assist another Company A SAP facility prepare for a government compliance inspection. During this visit, she completed Company A's internal inspection and drafted an SOP for the management of classified information at the facility. Her daughter was born later that year. (Tr. 76-79)

In May 2022, on her return from maternity leave, Applicant was again promoted and placed in charge of coordinating security for seven laboratories. In May 2023, she received an in-grade promotion because of her successful management of security relating to these projects. Later that year, she traveled to support a SAP corporate review. (Tr. 78-82)

In April 2024, Applicant successfully managed the breakdown of a classified laboratory. She coordinated the segregation of classified and unclassified items and the transportation of sensitive materials to other facilities. While her responsibilities within Company A increased over time, she believed she had found a balance in her workload. (Tr. 79-85)

However, Applicant experienced another security incident about three months later. This incident was of a different nature than previous events, and involved more complex circumstances, so it requires more in-depth discussion.

In July 2024, while preparing for multiple classified meetings involving government clients, Applicant worked in a small, classified space with several Company A vice presidents and program managers. She received an email over the company's classified server from a senior program manager requesting that she verify visitors badges for a classified meeting that was to occur a few days later. The email was marked as classified (top secret) and named a specific SAP alongside an attendance roster. No specific information about the SAP was contained in the email. Having regularly handled this type of information, Applicant believed the information should be unclassified so long as there was compartmentalization and certain handling limitations were in place specific to SAPs. Applicant also knew that the program manager who sent this email regularly overclassified information. Lacking workspace in the secured area, she printed the email, pen-marked and downgraded the classification of the email from top secret to unclassified with SAP handling protocols. She then took the downgraded email to her desk to complete the task. Applicant was within her authority to downgrade the classification of the document but admitted she had not previously downgraded classified information. She completed the task and placed the document in a folder on her desk. (Answer; GX 1,4; Tr. 81-98)

The next day, Applicant prepared other documents for an unrelated and unclassified training seminar. She scanned several unclassified documents and sent them, via email, to a colleague over Company A's internal unclassified server. The colleague also held top secret clearance and had been read into several SAPs. When she received the email, Applicant's colleague immediately responded and asked why Applicant had sent the sensitive SAP information over the unclassified server. Applicant then realized that the printed email she had downgraded the day prior was inadvertently attached to the materials she had scanned and sent over the unclassified server (SOR ¶ 1.a). (Answer; GX 1,4; 81-85)

Applicant immediately contacted her supervisor, Mr. V, as the mistaken transfer of sensitive SAP information over an unclassified server qualified as a security incident. Recognizing the SAP at issue, Mr. V suspected that the email should have at least been classified as secret. He based this on information he had received in a prior meeting he had with two government clients that Applicant did not attend. After consultation, the second government client (GC # 2) concluded that the information in the email at issue was classified as secret. As the material had been transmitted over an unclassified server, this was considered a data spill and a security violation by Applicant as the compromise of classified information could not be ruled out even though the email went between two people who maintained security clearances and had SAP access. (Answer; GX1,4; Tr. 85-100)

On reflection of the July 2024 incident, Applicant testified that she should have sought out a second opinion about whether to downgrade the email before proceeding and verified information with the government clients involved. She has not downgraded any classified information since this event. She also acknowledged that she made a mistake in grouping the email with other unclassified information and in transmitting it over an unclassified email system. (Answer; GX 1,4; Tr. 85-100)

Considering the obligations of a security officer in handling and protecting classified information, Applicant acknowledged there are a lot of rules in relation to her work. "I appreciate the rules. They create boundaries and guidelines to follow for myself, for program managers and engineers. Without rules, it would be a free-for-all and that wouldn't be good." She also recognized that, earlier in her career, she took on too many assignments as she did not want to "look bad or lazy." She now believes she has the confidence to speak up about her workflow and request assistance from her supervisors when needed. (Tr. 71-76)

Following the July 2024 incident, GC # 2 suspended Applicant's SAP access. However, she maintained her top-secret clearance. Company A removed her from working as a CSSO with SAPs. After about a month, she was reassigned to perform similar duties for classified collateral programs. She has not experienced any additional security incidents. (Tr. 92-103)

Later in 2024, Applicant's supervisors nominated her to chair Company A's security education committee, which is tasked with reviewing and updating training materials and coordinating monthly calls with various security professionals. She is also a member of a committee within Company A tasked with reviewing security incidents. In this capacity, she makes recommendations regarding any security incidents involving classified information outside of SAPs. (Tr. 95-111)

Applicant detailed the annual training she continues to receive. She noted that Company A changed a lot of procedures surrounding the opening and closing of classified spaces in 2020 including increased documented retraining and she has assisted in that process. (Tr. 105-110)

Two witnesses, Mr. V and Mr. R, testified on Applicant's behalf after previously submitting character letters in her support. Mr. V is a senior security manager at Company A and a master sergeant in the Marine Corps Reserve who has held security clearances for most of his military and civilian careers. He first met Applicant in 2018 and noted she has a reputation for being a very hard worker and always exceeding expectations. He highlighted that Applicant's work requires that she handle classified information across several projects every hour of every day. Regarding the security incidents in 2019, Mr. V believed that Applicant was "significantly mismanaged" and overworked, which led to the security infractions. Applicant began working on his team in October 2020 and he remained her supervisor until she was reassigned following the loss of her SAP access in 2024. Mr. V found Applicant's work to be "phenomenal" and that she "still would be

working on my team today based on the totality of her history, just based on her integrity, her honesty, her work ethic, [and] the value that she brings to the team." (Answer; Tr. 118-124)

Regarding the April 2024 security incident, Mr. V stated that Applicant had training as a derivative classifier and "absolutely [had] the authority to reclassify" information she believed was overclassified. However, the government client ultimately controlled the classification of the SAP at issue and determined that the information remained classified. He described the changes Company A made once the government client stated a higher classification of the information was necessary. When Applicant accidently included the email in paperwork that she scanned and sent to a colleague for an unclassified briefing, a security violation occurred. Mr. V highlighted that, when the issue was discovered, Applicant immediately brought it to his attention and communicated directly with the appropriate government clients. Once a security violation was assessed, Mr. V noted that Applicant responded favorably to the changes made within Company A. (Tr. 124-142)

Mr. V detailed that, once Applicant's SAP access was suspended, she continued working with top secret collateral information and supported Company A's facility security staff with operations and compliance. He noted that she has not experienced any security incidents since June 2024. He said, "she takes the security discipline and function with high regard. She gives it due diligence and believes in what we do as security professionals." He believes that Applicant continually demonstrates the reliability, trustworthiness and judgment necessary to maintain a security clearance. (Tr. 133-148)

Mr. R also testified on Applicant's behalf. He served twenty years in the Air Force before retiring in 2005. He then worked with Company A from 2005 until retiring in early 2026. He held security clearances for most of his military and professional career. He first met Applicant in 2018 when he was a SAP security manager. In review of Applicant's early career, Mr. R believed it was "not uncommon" for an employee new to the SAP environment to experience security infractions. He stated:

> The environment is fast-paced, it's dynamic. A security professional, almost right out of the gate, could be responsible for opening five to six facilities in a day, validating accesses for a meeting that might have 100 people showing up to it, [several] different programs, transmitting classified information, just about everything that they do on a daily basis involves touching, validating classified information.

Mr. R also noted that most of Applicant's training occurred "on the job," and that Company A had since formalized much of that training. He believed that, once Applicant's circumstances changed in 2019, "she went five years with not so much as a security infraction. … [To] have a security professional doing the work that [Applicant] was doing, again, touching classified every day, to go five years without so much as an infraction, … that's noteworthy." (Answer; Tr. 152-157)

Mr. R further commented that Applicant had "a good eye for process, and top-secret accountability is one of the most important things we do." He detailed that, on several occasions, Applicant worked to standardize Company A's processes for handling classified information and assisted in drafting SOPs. Even after the June 2024 security incident, Mr. R believed that Applicant was "top notch" and that he would "hire her again in a second. … [H]aving [Applicant] on the security team only strengthens it." (Tr. 158-167)

In addition to the letters and supporting testimony from Mr. V and Mr. R, Applicant submitted five reference letters from current and former colleagues at Company A. These individuals were all aware of the incidents referenced in the SOR and consistently spoke to Applicant's professionalism, integrity and maintenance of high ethical standards. They all believe that Applicant maintains a strong commitment to the safeguarding of classified and sensitive information and exercises the trustworthiness, reliability and judgment necessary to hold a security clearance. Applicant's employment record reflects that she received numerous awards and consistently received marks for high performance. (Answer)

Policies

It is well established that no one has a right to a security clearance. As the Supreme Court held in *Department of the Navy v. Egan*, "the clearly consistent standard indicates that security determinations should err, if they must, on the side of denials." 484 U.S. 518, 531 (1988)

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines. In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are used in evaluating an applicant's eligibility for access to classified information.

These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, these guidelines are applied in conjunction with the factors listed in the adjudicative process. The administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. According to AG ¶ 2(a), the entire process is a conscientious scrutiny of a number of variables known as the "whole-person concept." The administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable, in making a decision.

The protection of the national security is the paramount consideration. AG ¶ 2(b) requires that "[a]ny doubt concerning personnel being considered for national security eligibility will be resolved in favor of the national security." In reaching this decision, I have drawn only those conclusions that are reasonable, logical, and based on the evidence

contained in the record. Likewise, I have not drawn inferences grounded on mere speculation or conjecture.

Under Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, an "applicant is responsible for presenting witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel and has the ultimate burden of persuasion to obtain a favorable security decision."

A person who seeks access to classified information enters into a fiduciary relationship with the Government predicated upon trust and confidence. This relationship transcends normal duty hours and endures throughout off-duty hours. The Government reposes a high degree of trust and confidence in individuals to whom it grants access to classified information. Decisions include, by necessity, consideration of the possible risk the applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation of potential, rather than actual, risk of compromise of classified information.

Analysis

Guideline K, Handling Protected Information

The security concern for handling protected information 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.

Security violations "strike at the heart of the industrial security program" and require strict scrutiny. ISCR Case No. 21-00363 at 4 (App Bd. Jan 24, 2023); ISCR Case No. 14-05127 at 9 (App. Bd. June 24, 2016). Security violations are one of the strongest possible reasons for denying or revoking access to classified information. *See* ISCR Case No. 03-26888 at 1 (App. Bd. Oct. 5, 2006).

I have considered the disqualifying conditions for handling protected information under AG ¶ 34 and the following are potentially applicable:

> (a) deliberate or negligent disclosure of protected information to unauthorized persons, including, but not limited to, personal or business contacts, the media, or persons present at seminars, meetings, or conferences;
>
> (b) collecting or storing protected information in any unauthorized location;

(c) loading, drafting, editing, modifying, storing, transmitting, or otherwise handling protected information, including images, on any unauthorized equipment or medium;

(e) copying or modifying protected information in an unauthorized manner designed to conceal or remove classification or other document control markings;

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

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

Applicant's admissions, testimony and record evidence establish security concerns under AG ¶¶ 34(g) and 34(h) for all the allegations contained in the amended SOR. Additionally, AG ¶ 34(a) is established for SOR ¶ 1.d as this instance involved Applicant's disclosure of specific SAP information to an individual who was not authorized to receive it. AG ¶ 35(b) is established for SOR ¶¶ 1.b and 1.c as Applicant's failures to properly secure sensitive and classified information at the end of her workday reflects unauthorized storage of protected information. AG ¶ 35(c) is established for SOR ¶ 1.a as Applicant placed classified information on an unclassified server. However, AG ¶ 34(e) is not established for SOR ¶ 1.a as Applicant had authority to declassify the information at issue and when she did so, she did not proceed in a manner designed to conceal the removal of document control markings.

When it is established that an applicant has committed security violations, they have a "very heavy burden" in demonstrating mitigation. ISCR Case No. 14-05794 at 5 (App. Bd. July 7, 2016). Once a security violation or infraction has been established, the administrative judge must give any claims of reform or rehabilitation "strict scrutiny." ISCR Case No. 14-05127 at 8 (App. Bd. June 24, 2016). However, given the unique position of employers as actual administrators of classified programs and the degree of knowledge possessed by them in any particular case, their determinations and characterizations regarding security violations are entitled to considerable deference and should not be discounted or contradicted without a cogent explanation. *See* ISCR Case No. 20-00230 at 3 (App. Bd. Dec. 10, 2021); ISCR Case No. 19- 02136 at 3 (App. Bd. Mar. 8, 2021). The extent that an applicant accesses classified or sensitive information after prior security violations is relevant in determining whether the applicant has demonstrated rehabilitation and increased security awareness. *See* ISCR Case No. 04-12742 at 3 (App. Bd. Feb. 25, 2011).

I have considered the mitigating conditions under AG ¶ 35, and the following are potentially applicable:

(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.

Applicant started working with a Company A subcontractor in 2008. She began supporting the company's security department in 2011 and was hired by Company A directly as a security representative in 2014. Since then, she has excelled and built a career at Company A managing personnel security, physical security and information security around multiple SAPs and classified programs. Her work consistently involved performing numerous tasks relating to the management of classified and protected information every hour of every day. Some of her colleagues considered her a subject matter expert in security.

Applicant's experience has not come without a learning curve. Between October 2015 and July 2018, she experienced four security incidents after she failed to properly secure areas containing classified information. Each time she accepted responsibility, received training, and made changes to how she managed her workflow. She then openly shared her experiences with colleagues and new employees during company training sessions so that they would not make similar mistakes.

During that time, Applicant received multiple promotions, and her responsibilities grew. She also reflected on her own experiences and assisted in revamping several aspects of the training that Company A employees received regarding security management and access to classified programs.

As she excelled at work, Applicant took on more obligations. She admitted that, early in her career, she did not want to "look bad or lazy" and took on too many assignments. Throughout most of 2018, she felt that she was doing the job of three people and expressed concerns to her superiors. She was told that help was coming. Meanwhile, the hectic pace of her work caught up to her and she experienced four security incidents in 2019. The most notable of these incidents occurred when she inadvertently provided information about a SAP to an individual who was not cleared into that program. Applicant accepted responsibility for her error and assisted Company A in making procedural changes so that a similar error would not occur.

Shortly after these events, Applicant and her superiors recognized that her workload was leading to errors in her management of security operations. She changed positions within Company A and quickly exceeded expectations in fulfilling her new obligations. Additionally, she helped train other security professionals, drafted SOPs and managed government compliance inspections. She continued to actively manage classified information for five years before experiencing another security incident.

In July 2024, Applicant committed a security violation when she downgraded a document containing classified SAP information to unclassified with SAP handling protocols and then inadvertently scanned and emailed that information to a colleague over an unclassified server. Once she discovered the error, she immediately reported the incident to her supervisor and the government client. While Applicant had the authority to downgrade the classification of documents, the relevant government client later confirmed that the information should have remained classified. Although unintentional, this constituted a data spill and was categorized as a compromise of information. Applicant accepted responsibility for the incident. When the government client suspended her SAP access, she accepted a new position within Company A and continues to handle classified information daily.

Applicant also chairs Company A's security education committee and continues to update training materials. She sits on a committee charged with reviewing security incidents across Company A and makes recommendations regarding reporting and mitigation of those incidents. She continues to regularly coordinate with security professionals and provides training for new employees. She had not experienced another security incident since July 2024. Her previous supervisors spoke highly of her and detailed that she exercises the judgment, reliability and trustworthiness necessary to maintain a security clearance.

In review of the mitigating factors, AG ¶ 35(a) is fully applicable to SOR allegations ¶¶ 1.b through 1.i involving security incidents from 2015 through 2019. These events occurred several years ago. Applicant accepted responsibility and made substantive changes to how she managed her daily interaction with classified information. AG ¶ 35(a) is also applicable to SOR ¶ 1.a as the July 2024 incident happened under unusual circumstances and Applicant has established it is unlikely to recur. AG ¶ 35(b) is fully applicable to all the SOR allegations as Applicant has consistently responded favorably to counseling and security training. Even further, she has reflected on her own security incidents to improve the training of other employees within Company A. Those that work with her consistently state that she respects the rules in securing classified information and maintains the highest degree of professionalism in the discharge of her security responsibilities.

While Applicant reflected on some of the shortcomings she experienced in her training as a security officer, she refused to blame those shortcomings for her security incidents. Instead, she used her experiences to improve the training of others. Additionally, regarding the July 2024 incident, there were aspects in the management of

the SAP material at issue that were unclear to Applicant. Had she been fully aware of the sensitivity involved, she would not have downgraded the classification of the email. AG ¶ 35(c) is partially applicable to the SOR allegations.

AG ¶ 35(d) is fully applicable to SOR ¶¶ 1.b through 1.i as the security incidents were inadvertent, promptly reported and there is no evidence of a compromise of information. AG ¶ 35(d) is only partially applicable to SOR ¶ 1.a as, with the transmission of classified information over an unclassified server, the compromise of classified information could not be ruled out, resulting in a security violation against Applicant. Nonetheless, Applicant's actions were inadvertent and not reflective of a pattern of conduct.

In evaluating the mitigating conditions under Guideline K, I reviewed the cumulative record and applied strict scrutiny in accordance with Appeal Board caselaw, holding Applicant to a high burden of persuasion. I had the opportunity to observe Applicant's demeanor during her hearing and found that she was credible and candid. She addressed the security incidents in detail, accepted responsibility and noted changes she made after each incident. She takes her responsibilities as a security officer seriously. Furthermore, the record reflects that she has sustained a high level of performance since first working with Company A, including more than a decade of daily, direct responsibility for safeguarding classified information. Considering the totality of the circumstances, Applicant has mitigated the security concerns related to the handling of protected information.

Whole-Person Concept

Under the whole-person concept, the 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. The 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.

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. 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.

Those who know Applicant in the workplace state that she maintains the highest degree of professionalism and integrity. The record evidence supports this assessment. As a security officer, she is tasked daily to navigate a broad array of rules and regulations in maintaining the protection of classified and sensitive information. From 2015 through 2019, she experienced several security infractions that were similar in nature (setting an alarm, spinning a lock, properly securing a file at the end of a workday). While she took responsibility for these incidents, they were at least partially attributable to minimal training and being overworked. The security incident in July 2024 was serious and determined to be a security violation. It was also inadvertent, isolated, properly and immediately reported, and remedied by subsequent training. With full knowledge of these events over Applicant's career, Company A continues to maintain high confidence in her abilities and has promoted her on multiple occasions. She has demonstrated that she is a dedicated security professional.

Applicant has met her significant burden to mitigate the Guideline K security concerns and has established that she can maintain the judgment, trustworthiness and reliability necessary to hold a security clearance. The record evidence leaves me without questions or doubts about her eligibility and suitability for a security clearance. I conclude Applicant mitigated the security concerns.

Formal Findings

Formal findings for or against Applicant on the allegations set forth in the SOR, as required by section E3.1.25 of Enclosure 3 of the Directive, are:

Paragraph 1, Guideline K:	FOR APPLICANT
Subparagraphs 1.a – 1.i:	For Applicant

Conclusion

In light of all of the circumstances, it is clearly consistent with the national interest to grant Applicant a security clearance. Eligibility for access to classified information is granted.

_____
Bryan J. Olmos
Administrative Judge