DEPARTMENT OF DEFENSE
DEFENSE LEGAL SERVICES AGENCY
DEFENSE OFFICE OF HEARINGS AND APPEALS
APPEAL BOARD
POST OFFICE BOX 3656
ARLINGTON, VIRGINIA 22203
(703) 696-4759

Date: May 12, 2023

In the matter of:	)	
-----	)	USAF-C Case No. 22-02263-R
Applicant for Security Clearance	)	

APPEAL BOARD DECISION

APPEARANCES

FOR GOVERNMENT
James B. Norman, Esq., Chief Department Counsel

FOR APPLICANT
Christopher Snowden, Esq.

On May 23, 2022, the Department of Defense (DoD) issued a statement of reasons (SOR) pursuant to DoD Manual 5200.02 (Apr. 3, 2017, as amended) (DoDM 5200.02) advising Applicant that her conduct raised security concerns under Guideline E (Personal Conduct), Guideline K (Handing Protected Information), and Guideline M (Use of Information Technology) of the National Security Adjudicative Guidelines. On July 20, 2022, Applicant submitted a response to the SOR.

On October 4, 2022, DoD Consolidated Adjudication Services (CAS) revoked Applicant's eligibility for access to classified information, and she appealed that revocation under the provisions of DoDM 5200.02. On December 2, 2022, Under Secretary of Defense (Intelligence and Security) Ronald Moultrie issued a memorandum that DoD civilian and military personnel whose clearance eligibility was revoked or denied between September 30, 2022, and the date of that memorandum, shall be provided the opportunity to pursue the hearing and appeal process as set forth in DoD Directive 5220.6 (Jan. 2, 1992, as amended) (Directive).

As a result of Secretary Moultrie's memo, Applicant was given the opportunity to receive the process set forth in the Directive, and she elected that process. On March 16, 2023, after conducting a hearing, Defense Office of Hearings and Appeals (DOHA) Administrative Judge Jennifer I. Goldstein denied Applicant's request for a security clearance. Applicant appealed pursuant to Directive ¶¶ E3.1.28 and E3.1.30. For reasons stated below, we affirm the Judge's decision.

Findings of Facts and Conclusions

Applicant, who is in her 40s, served as a general engineer in her most recent employment from which she medically retired in December 2022. Appeal Brief at 1. The SOR alleged that she has a history of workplace misconduct spanning four separate employers. In her analysis, the Judge summarized the significant facts of the case as follows:

Guideline E (Personal Conduct)

> From 2012 through 2022, Applicant's employment-related conduct demonstrated a history of questionable judgment, untrustworthiness, unreliability, lack of candor, and unwillingness to comply with rules and regulations. First, while employed by the Navy from 2011 to 2013, she received a letter of caution for failing to follow her supervisor's instructions and engaging in inappropriate behavior by alienating customers. She also violated base rules by bringing a cell phone into an area where cell phones were prohibited. Additionally, while working for Employer Three, Applicant was terminated for violating the employer's policy, demonstrating negligence, disruptiveness, unprofessionalism, and for interjecting herself into things not related to her job.
>
> Similarly, Applicant displayed this same type of conduct while working for Employer Five. From September 2021 through her suspension in September 2022, she blatantly disregarded the instruction of her supervisor at least 13 times. She was first counseled on her inappropriate and unprofessional behavior in September 2021. Despite counseling, she failed to bring work-related concerns to her supervisor as instructed in the counseling and sent multiple inappropriate emails to the entire staff. She repeatedly used her government email address to send messages related to areas outside of her employment duties, even after being explicitly instructed not to do so in writing at least four times. Her conduct, unrelated to her allegations of discrimination and retaliation, establishes a pattern of rule violations and demonstrates questionable judgment. [Decision at 20-21.]
>
> * * *
>
> Applicant's disregard of her employers' directions is well documented and has been reported repeatedly over her career. Further, her conduct is recent. While she acknowledged at least one instance of improperly using her government email to obtain the DTRA [Defense Threat Reduction Agency] report, she failed to take responsibility for her actions. She knew it was wrong to use her government email,

> yet she chose to do so repeatedly. Instead of accepting responsibility for her improper actions, she blamed others and claimed she was being retaliated against. Her conduct continues to reflect poorly on her judgment. [Decision at 21.]

Guideline K (Handling Protected Information)

> Applicant failed to follow the guidance of her supervisors when it came to handling protected information while employed by Employers Three and Five. While employed by Employer Three, she shared three proprietary documents in violation of the employer's policies. While at Employer Five, she committed a series of inappropriate actions with respect to protected information, including: compiling OSINT [open-source intelligence] against the direction of her supervisor; disseminating that compilation over an unclassified government email network; and not using the proper CUI [controlled unclassified information] markings on that documentation. [Decision at 22.]

None of the Guideline K mitigating conditions apply to Applicant's misconduct, which is recent and demonstrates a recurring pattern. Disregarding repeated attempts of her supervisors to provide her guidance, Applicant failed to comply with safeguards and failed to demonstrate a positive attitude toward discharging her security responsibilities.

Guideline M (Use of Information Technology)

> The evidence shows she misused her government email on multiple occasions including contacting DTRA, and that she disseminated OSINT that she collected. Applicant did so even though her actions were not part of her official duties, and she continued to do so even after she had been instructed by her supervisor to cease such activities. Applicant acknowledged improperly using her government email to contact DTRA. [Decision at 23.]

Applicant's misuse of her government email was unrelated to her assigned tasks. This conduct was a deliberate violation of her supervisor's directives to not engage in such activities using Government assets. Applicant made no good-faith effort to correct her conduct.

Discussion

Scope of Review

There is no presumption of error below, and the appealing party must raise claims of error with specificity, identify how the Judge committed factual or legal error, and cite to specific portions of the record supporting any alleged error. Directive ¶¶ E3.1.30 and E3.1.32. *See also* ISCR Case No. 02-12199 at 2 (App. Bd. Aug. 8, 2005). The Appeal Board does not review a case *de novo*. *Id.* Instead, our scope of review is narrow, and we may not substitute our judgment for that of the Judge. *See, e.g.,* ISCR Case No. 04-07766 at 2 (App. Bd. Sep. 26, 2006). More specifically, the Board's scope of review is limited to deciding whether: (1) the Judge's findings of fact are supported by substantial evidence, which is defined in the next section; (2) the Judge

complied with the procedures required by Executive Order 10865 and the Directive; and (3) the Judge's rulings or conclusions are not arbitrary, capricious, or contrary to law. Directive ¶ E3.1.32. A Judge's conclusions are often subjective in nature and are sustainable if they constitute reasonable inferences drawn from the evidence. *See, e.g.*, ISCR Case No. 17-02225 at 2-3 (App. Bd. Jun. 25, 2019). *See also* ISCR Case No. 02-12199 at 2 (setting forth the standard applied in analyzing whether the Judge's conclusions are erroneous). If an appealing party demonstrates factual or legal error, then the Board must consider whether the error is harmful or harmless; whether the Judge's decision can be affirmed on alternate grounds; and, if the Judge's decision cannot be affirmed, whether it should be remanded or reversed. *Id*. at 3. *See also* Directive ¶¶ E3.1.32 and E3.1.33.

Challenges to the Findings of Fact

At the outset, it is noted that Applicant's brief applies the wrong standard of proof in challenging the legal sufficiency of the Judge's findings of fact. In the beginning of her brief, Applicant correctly states that a Judge's findings of fact must be supported by "substantial evidence," *i.e.*, such "relevant evidence as a reasonable mind might accept as adequate to support a conclusion in light of all contrary evidence in the record." Appeal Brief at 3 and 10 (citing Directive ¶ E3.1.32.1). Applicant further states, "'Substantial evidence' is 'more than a scintilla but less than a preponderance.'" Appeal Brief at 10 (quoting *See v. Washington Metro. Area Transit Auth.*, 36 F.3d 375, 380 (4th Cir. 1994)). Several times, however, Applicant incorrectly applies the "preponderance of the evidence" standard in challenging the Judge's specific findings, which undercuts her arguments. Appeal Brief at 11, 14. At this point, it also merits noting that Directive ¶ E.1.32.1 provides the Appeal Board shall give deference to the Judge's credibility determinations in reviewing the findings of fact. In her decision, the Judge concluded that Applicant's "credibility is questionable." Decision at 25. Based on our review of the record, we find no reason not to defer to that credibility determination.

The Judge found that Applicant violated Employer Three's policy by sharing proprietary documents with the Government client. Decision at 5. Applicant contends that the Government presented insufficient evidence to show that she mishandled proprietary information. Appeal Brief at 5, 10-11, 13-14, 16. Applicant argues that proprietary information involves a property interest and that the Judge "provides no rationale for how the disclosures constituted a property interest of [Employer Three]." Appeal Brief at 11. We construe Applicant's argument as asserting that the Government failed to establish that the information in question was proprietary information. We do not find this argument persuasive.

At the hearing, Applicant offered into evidence documents that established she mishandled Employer Three's proprietary information. Applicant Exhibit (AE) 1-D. This included portions of a DoD Report of Investigation reflecting that Employer Three reported that Applicant "violated [its] policy by sharing [its] proprietary documents with the government client." *Id*. at 5. The Judge could rely on the company's representations that the information at issue was propriety information without having the company disclose the exact nature of that information or, as Applicant claims, prove it had a property interest in that information. As the Board has previously stated, we give deference to a company's findings and conclusions in its security investigations. *See, e.g.*, ISCR Case No. 15-08385 at 4 (App. Bd. May 23, 2018). In the classified information context, we have

stated that, "because of 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." ISCR Case No. 10-07070 at 8 (App. Bd. Apr. 19, 2012). The same reasoning applies to a company's determinations and characterizations regarding violations of its policies on the safeguarding and handling of sensitive information, such as propriety information. In this regard, the Judge was not required to accept Applicant's claim that no proprietary information was shared (SOR Response at 15) and instead had to weigh that claim in light of all the record evidence.

Applicant also contends that the Judge's conclusion that Applicant "compil[ed] OSINT against the direction of her supervisor; disseminat[ed] that compilation over an unclassified government email network and [failed to use] the proper CUI markings on that documentation" (Decision at 22) is contradicted by an earlier finding that – as summarized by Applicant – she only "*possibly* transmitted protected material." Appeal Brief at 11, 13, 14. This argument, however, misconstrues the relied-upon finding and conflates two issues: 1) that Applicant transmitted compiled material over an unclassified network without proper CUI markings; and 2) that by virtue of her compiling the material, even from open sources, she was potentially altering the classification status of the compilation. Contrary to Applicant's summarized finding, the Judge found that Applicant's command was concerned that she was compiling and sending OSINT information over an unclassified network and that "by adding her own analysis to the open-source intelligence, it is possible to elevate the classification level from what was unclassified open-source material to something of a higher classification." Decision at 9. Applicant appears to argue that, because the evidence establishes only that she *possibly* altered the classification status of various material through her compilation, the Government failed to establish that her transmission of the material over an unclassified network was improper. This conclusion does not follow. The Judge's finding about the possible elevation of classification status of compiled open-source material is well supported by the record, as is that Applicant was repeatedly instructed to stop compiling and transmitting such material over an unclassified network, and that she disregarded those instructions. *See* Tr.-1 at 61-62, 86-87, 123-124; Government Exhibit (GE) 8 at 1; GE 9 at 1; GE 10 at 1; GE 14; AE 1-A at 326. We find no error in the Judge's findings or conclusions that followed.

Applicant failed to show that any of the Judge's findings of fact were defective. From our review of the record, the Judge's material findings of a security concern are based on substantial evidence or constitute reasonable inferences that could be drawn from the evidence. *See, e.g.*, ISCR Case No. 17-02225 at 2-3.

Challenges to the Conclusions

Applicant's brief claims that the Judge erred in failing to comply with the provisions in Executive Order 10865 and the Directive by not considering all the evidence and by not properly applying the mitigating conditions and whole-person concept. These arguments amount to a disagreement with the Judge's weighing of the evidence, which is a matter within the Judge's special province. *See, e.g.*, *Inwood Laboratories, Inc. v. Ives Laboratories Inc.*, 456 U.S. 844, 856 (1982). As the trier of fact, the Judge must use commonsense in evaluating the evidence and

consider the record as a whole. Directive ¶ 6.3 and Encl. 2, App. A ¶ 2(c). The Judge is responsible for resolving conflicts in the evidence and has discretion in weighing the evidence, both favorable and unfavorable. In analyzing the evidence, a Judge is not required to accept unrebutted testimony or other evidence uncritically or without considering it in relation to all relevant and material evidence in the record. *See, e.g.*, ISCR Case No. 98-0265 at 4, n. 2 (App. Bd. Mar. 17, 1999).

An appealing party's lengthy or strong disagreements with the Judge's conclusions and whole-person analysis are not necessarily sufficient to demonstrate error. To establish error, an appealing party must demonstrate the Judge's analysis or conclusions were arbitrary, capricious, or contrary to law. Directive ¶ E3.1.32.3.

In her brief, Applicant raises several challenges to the Judge's analysis and conclusions. For example, Applicant argues that the Judge did not place appropriate weight on her character evidence, including individuals who stated that Applicant was not difficult to work with; that she was the target of attacks by people who were much less qualified; and that she was dismissed for trying to follow the regulations. She further claims that she was not provided appropriate training on OSINT and the proper channels for disseminating that information. In essence, Applicant is advocating for an alternative weighing of the evidence. The existence of mitigating evidence, however, does not alone compel the Judge to make a favorable security clearance decision. In weighing the evidence, the Judge must decide whether the favorable evidence outweighs the unfavorable evidence, or *vice versa*. A party's disagreement with the Judge's weighing of the evidence, or an ability to argue for a different interpretation of the evidence, is not sufficient to demonstrate the Judge weighed the evidence or reached conclusions in a manner that is arbitrary, capricious, or contrary to law. *See, e.g.,* ISCR Case No. 19-01431 at 4 (App. Bd. Mar. 31, 2020).

Based on our review, we conclude that none of Applicant's arguments are sufficient to rebut the presumption that the Judge considered all of the record evidence or to demonstrate the Judge weighed the evidence in a manner that was arbitrary, capricious, or contrary to law. *See, e.g.*, ISCR Case No. 21-01169 at 5 (App. Bd. May 13, 2022). Furthermore, contrary to Applicant's assertions, we also conclude that the Judge's whole-person analysis satisfies the requirements of Directive ¶ 6.3, in that the Judge evaluated Applicant's security-significant circumstances in light of the entirety of the record evidence. *See, e.g.,* ISCR Case No. 14-02806 at 4 (App. Bd. Sep. 9, 2015).

Claim of Reprisal for Whistleblowing

Applicant's brief asserts that adverse actions were taken against her, including the attempt to revoke her security clearance, because she voiced concerns over safety hazards, violations of regulations, and discrimination. She further states that "the process to revoke a security clearance was never meant to circumvent legitimate methods of adjudicating employment disputes." Appeal Brief at 1.

Presidential Policy Directive-19 and 50 U.S.C. § 3341(j) provide protections to cleared Federal Government employees who are whistleblowers. These protections are implemented in DoDM 5200.02, which provides:

7.3. PROHIBITION ON RETALIATION BY AFFECTING ELIGIBIILLTY FOR ACCESS TO CLASSIFIED INFORMATION.

> a. It is strictly prohibited to take, fail to take, or threaten to take or fail to take any action affecting an individual's eligibility for access to classified information as a reprisal for a protected disclosure of fraud, waste, or abuse pursuant to Presidential Policy Directive/PPD 19.
>
> b. Employees may appeal actions affecting eligibility for access to classified information allegedly taken as a reprisal for a protected disclosure of fraud, waste, or abuse in violation of Presidential Policy Directive/PPD 19.
>
> c. All personnel security adjudicators, DOHA administrative judges (AJs), and Personnel Security Appeals Boards (PSABs) will, as part of their adjudication of an individual's eligibility, consider and resolve any claims of reprisal for whistleblowing.

PPD-19 ¶ F(5) defines "Protected Disclosure" as an employee's disclosure to a supervisor in his or her chain of command, an Inspector General, or certain other officials of information that he or she "reasonably believes evidences (i) a violation of any law, rule, or regulation; or (ii) gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety" as well as other disclosures identified in that Directive. Under 50 U.S.C. § 3341(j)(4)(C), a Federal agency shall find a retaliation violation if the protected disclosure "was a contributing factor in the adverse security clearance or access determination taken against the individual, unless the agency demonstrates by a preponderance of the evidence that it would have taken the same action in the absence of such disclosure, giving the utmost deference to the agency's assessment of the particular threat to the national security interests of the United States in the instant matter." *See also* Security Executive Agent Directive 9, Appellate Review of Retaliation Regarding Security Clearance and Access Determinations.

In her decision, the Judge reviewed Applicant's whistleblower-reprisal claims to determine whether they may have been a contributing factor in the review of her security clearance eligibility. After first identifying Applicant's various whistleblower reprisal complaints, the Judge concluded:

> [E]ven if those complaints were true, based on the entire record, I am satisfied that the DOD CAS would have acted on [Applicant's] security clearance in the absence of her complaints. Her failure to follow supervisory instructions at Employers One and Five, conduct unbecoming of a federal employee, inappropriate behavior in the workplace of Employers Three and Five, and unapproved volunteer activity on government time while working for Employer Five are sufficient to establish, by a preponderance of the evidence, that the SOR would have been issued in the absence of her complaints. Her protected disclosures were not contributing factors in the adverse security access determination. [Decision at 26-27.]

In this regard, it merits noting that Applicant's transmissions of OSINT over the command's unclassified computer network was one of several key security concerns that led to

the review of her security clearance eligibility. At the hearing, Applicant testified that she was involved in "gray space" or "gray operations," which she explained was operating "in between lines of official versus unofficial" actions. Tr.-3 at 123; AE 27; Decision at 2-3. Some of her "gray operation" activities included supplying data to military intelligence groups, helping to map flight paths, and assisting individuals with visas to come to the United States from a war-torn country. *Id*.

The record evidence sets forth several instances in which Applicant transmitted OSINT unrelated to her official responsibilities over the command's unclassified computer network in violation of supervisory instructions, directions, and orders. Some notable events regarding this issue are summarized below.

a. On December 20, 2021, Applicant was issued a letter of reprimand, in part, for misusing her Government email account by sending emails unrelated to her professional duties. These emails concerned container ships entering the United States. In one of those emails, Applicant indicated that she knew individuals who could assist in conducting reconnaissance of these ships. Decision at 9-11; GE 4 at 2; GE 7 at 1.

b. On February 16, 2022, Applicant sent an email to her supervisor, an intelligence officer, and other senior members of Employer Five over the command's unclassified network that discussed hypersonic threats at certain locations outside the United States. Decision at 12. In a related memorandum for the record, Applicant's supervisor noted that Applicant is not assigned to the intelligence field, that intelligence professionals within the command expressed concerns about Applicant transmitting "threat assessments" over the unclassified network, and that they recommended she confine such transmissions to the classified network. GE 8 at 1. The day after receiving Applicant's email, her supervisor replied and instructed Applicant to refrain from sending such emails over the unclassified network "to mitigate classification, OPSEC [operational security], and OSINT concerns." *Id.* Based on her supervisor's email, Applicant should have understood that transmitting OSINT over the unclassified network with her comments or analysis raised issues about whether such actions elevated that information to the level of classified information and, thereby, created a security violation. Approximately five minutes after her supervisor's response, Applicant replied by stating the information was gathered from open sources. *Id*. About three hours later, Applicant disobeyed her supervisor by sending an email regarding a country involved in a military conflict; however, she did not include her supervisor on that email. *Id*. Shortly after receipt of this latter email, an intelligence officer replied directly to Applicant, noting that her email's contents should have been restricted to the classified network, her comments were not related to the command's mission, and, if collection of open-source intelligence was required, specially trained OSINT professionals would perform that function. In the memorandum for the record, her supervisor indicated that Applicant's conduct was unacceptable and posed a potential threat to national security. *Id.* at 2.

c. On February 24, 2022, the command's Operations Director notified Applicant that her access to classified information was being suspended. GE 9. Of note, the Operations Director was neither in Applicant's chain of command nor apparently involved in any of her protected disclosures. The Operations Director's memorandum indicated that the suspension was based on various instances of Applicant's questionable conduct, including her transmission of OSINT over

the command's unclassified network. The Operations Director also notified her that an incident report must be submitted to DoD CAS, that he was taking that action in his capacity as the Security Program Executive, and that DoD CAS would make a final determination concerning her security clearance eligibility. *Id*.

d. Despite being directed by her supervisor and an intelligence officer not to transmit OSINT over the unclassified network and being advised by the Operations Director that her access to classified information was suspended, in part, for making such transmissions, Applicant again used the command's unclassified network for the transmission of OSINT. On March 30, 2022, Applicant's supervisor sent her a memorandum that directed her to cease and desist using her "government electronic mail (email) account to collect, transmit, compile, consolidate or otherwise redistribute open source intelligence . . . information, and tactical information." GE 10 at 1. This memo advised her that she is not an intelligence officer and that her responsibilities did not require her to engage in open-source intelligence gathering, analysis, or transmission. It was issued after her supervisor became aware that Applicant sent two emails on her Government computer on March 3, 2022, that were unrelated to her official duties. These emails were apparently sent in her unofficial "gray operation" role. One of them asked a DTRA contractor to send her information about a power plant fire in a country involved in a military conflict. Her supervisor's memo noted that their command's mission did not involve getting DTRA intelligence products to end users and that Applicant's use of her official Government email in making that request created the impression that her request was part of her official duties. *Id*.

e. On May 2, 2022, Applicant sent an email regarding hypersonics that contained an excel spreadsheet and other documents. This email resulted in Applicant's government computer, as well as those of 17 other employees, being seized so that a review could be conducted to determine whether her email created a spillage of classified information over the unclassified network. Decision at 15; AE 1-A at 326. Due to this incident, Applicant's access to DoD networks, DoD information technology assets, and common access card were suspended. Decision at 15. It also resulted in Applicant's supervisor and the Director of Information Production issuing her a cease-and-desist order on May 18, 2022, prohibiting Applicant from communicating hypersonic information in any format. AE 1-A at 326. The official review of this potential spillage incident later determined that Applicant's email contained only CUI and should have been marked accordingly. Decision at 17; GE 14.

f. On May 31, 2022, Applicant's supervisor issued her a directive that prohibited her from using government-duty time or government resources for intelligence collection, transmission, or related activities. This directive was generated after Applicant sought contact information on intelligence personnel so that she could pass along a tip concerning Taliban activity. AE 1-E at 321. Applicant violated this directive on June 23, 2022, when she approached an official within her division to inform him that she had intelligence information on foreign nationals and possibly U.S. persons that required urgent attention, showing him images of passports on her cell phone. Decision at 16.

Applicant's contention that the actions taken to revoke her security clearance were in retaliation for her being a whistleblower is not supported by the evidence. Besides her bare reprisal assertion, she failed to provide any specifics about that claim. In particular, she does not explain

her basis for believing a reprisal occurred, does not highlight any portions of the record evidence that would support her claim, and does not assert that the Judge committed any factual or legal error in making findings of fact or conclusions regarding this issue.

We agree with the Judge's conclusion regarding Applicant's reprisal claims. Based on our review of the record, we conclude that Applicant's purported protected disclosures were not a contributing factor in the initiation of the actions taken to revoke her security clearance eligibility or in the ultimate unfavorable security clearance determination. Furthermore, a preponderance of the evidence in this case demonstrates that DoD would have taken action to revoke Applicant's security clearance eligibility even if her protected disclosures were a contributing factor in the initiation of the review of her clearance eligibility.

Conclusion

Applicant has a history of employment-related misconduct at four employers, including both private companies and the Federal Government, between 2012 and 2022. This misconduct is well documented. The record evidence sufficiently establishes that she has engaged in a pattern of inappropriate workplace behavior, such as failing to follow instructions, interjecting herself into matters that did not involve her, making threatening or disparaging comments, engaging in disruptive behavior, and exhibiting conduct unbecoming a Federal employee. For example, Applicant claimed a commanding officer's executive assistant had threatened her life in 2013, but an ensuing investigation found that Applicant's allegations were unsubstantiated and "were specifically repudiated and contradicted by the collective weight of the statements of ten witnesses." Decision at 4 (quoting AE 1-B at 245). Applicant's employment history also reveals that she was terminated from a fifth job with a state government, although there is no SOR allegation pertaining to that employment. She has repeatedly claimed that corrective or disciplinary actions taken by employers were reprisals against her for being a whistleblower; however, she has not shown that any of those claims were substantiated by appropriate investigating authorities. Particularly troubling is her use of Government resources to engage in intelligence gathering activities for her unofficial "gray operations," and her failure to follow official orders related to such unofficial activities. She mishandled proprietary information while working at Employer Three. Her conduct demonstrates that she was unwilling to comply with supervisory instructions, directions, or orders, which raises doubts about her willingness to follow rules, regulations, and supervisory orders regarding the protection of classified or sensitive information. In general, Applicant's misconduct is recent, frequent, and raises security concerns about her trustworthiness, reliability, and good judgment. The ultimate burden of persuasion was on Applicant to obtain a favorable clearance decision. Directive ¶ E3.1.15. We agree with the Judge that Applicant failed to mitigate the alleged security concerns. In particular, she failed to show that her various types of workplace misconduct are unlikely to recur.

Applicant failed to establish that the Judge committed any harmful error or that she should be granted any relief on appeal. The Judge examined the relevant evidence and articulated a satisfactory explanation for the decision. The decision is sustainable on the record. "The general standard is that a clearance may be granted only when 'clearly consistent with national security.'" *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). *See also*, Directive, Encl. 2, App. A

¶ 2(b): "Any doubt concerning personnel being considered for national security eligibility will be resolved in favor of the national security."

Order

The decision is **AFFIRMED**.

Signed: James F. Duffy
James F. Duffy
Administrative Judge
Chair, Appeal Board

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

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