66 FLRA No. 56

UNITED STATES
NUCLEAR REGULATORY COMMISSION
(Agency/Petitioner)

and

NATIONAL TREASURY
EMPLOYEES UNION
(Labor Organization/Exclusive Representative)

WA-RP-10-0019

_____

DECISION AND ORDER
ON REVIEW

October 31, 2011

_____

Before the Authority: Carol Waller Pope, Chairman, and Thomas M. Beck and Ernest DuBester, Members[1]

I. Statement of the Case

This case is before the Authority on an application for review (application) filed by the Agency/Petitioner (Agency) under § 2422.31 of the Authority's Regulations.[2] The Labor Organization/Exclusive Representative (Union) filed an opposition.

The Agency filed a petition to clarify the bargaining unit status of twenty-four Criminal Investigators (CIs) of the Agency's Office of Investigation (OI). The Regional Director (RD) determined that twelve of the CIs should be excluded from the bargaining unit (unit) under § 7112(b)(6) of the Federal Service Labor-Management Relations Statute (the Statute) (§ 7112(b)(6)),[3] and that the remaining twelve CIs should be included in the unit. In an Order, the Authority granted the application and deferred action on the merits.

On review of the merits, and for the reasons that follow, we affirm the RD's Decision and Order in part, reverse it in part, and order the RD to take appropriate action consistent with this decision.

II. Background and RD's Decision

The Agency filed a petition alleging that the CIs in the OI should be excluded from the unit because they perform intelligence, counterintelligence, investigative, and security work that directly affects national security under § 7112(b)(6).

As an initial matter, the RD found that the Agency's mission is to "license and regulate the Nation's civilian use of nuclear power and materials to ensure the adequate protection of public health and safety, promote the common defense and security, and protect the environment." RD's Decision at 2. In this connection, the RD determined that the Agency licenses and/or regulates commercial nuclear power plants and fuel-cycle facilities that process uranium, and also regulates the use of nuclear materials by thousands of other entities throughout the country. *Id.* The RD stated that it was undisputed that the United States' commercial nuclear power plants and the use of nuclear materials constitute a part of the Nation's critical infrastructure, and he determined that any incapacity or destruction of these systems and assets would have a debilitating impact on security, the economy, and public health and safety. *Id.* at 12. Accordingly, the RD found that the Agency's work concerns national security within the meaning of § 7112(b)(6). *Id.*

Next, the RD addressed whether the CIs are engaged in investigative work that directly affects national security. In this connection, the RD found that OI investigates entities and individuals who allegedly have violated laws, regulations, and/or license conditions issued by the Agency, and that the CIs conduct

[1] Member Beck's dissenting opinion is set forth at the end of this decision.

[2] Section 2422.31(c) of the Authority's Regulations provides, in pertinent part, that

> (c) The Authority may grant an application for review only when the application demonstrates that review is warranted on one or more of the following grounds:
>
> (1) The decision raises an issue for which there is an absence of precedent; [or]
>
> . . . .
>
> (3) There is a genuine issue over whether the Regional Director has:
>
> (i) Failed to apply established law; [or]
>
> . . . .
>
> (iii) Committed a clear and prejudicial error concerning a substantial factual matter.

[3] Section 7112(b)(6) provides, in pertinent part, that the Authority shall not find a unit appropriate if it includes "any employee engaged in intelligence, counterintelligence, investigative, or security work which directly affects national security[.]" The RD excluded these twelve CIs on the ground that they access classified information. *See* RD's Decision at 14. As no application was filed with respect to these twelve CIs, we do not discuss them further.

investigations regarding: (1) material false statements (e.g., an individual failing to report his or her criminal history when applying for admission to a nuclear power plant, or a licensee falsely reporting that certain security training has been provided); (2) violations of other Agency regulations (e.g., alleged failures by licensees, applicants for licenses, and employees of contractors used by those entities to comply with prohibitions against the disclosure of information, or to comply with security plans and procedures designed to protect regulated facilities); (3) discrimination (i.e., claims that employees have been discriminated against for reporting safety problems at a nuclear power plant); and, upon request, (4) "assists to staff" (i.e., investigative assistance to Agency staff involving matters of regulatory concern that may not involve a specific indication of wrongdoing). *Id.* at 2-3.

The RD determined that the "vast majority of the investigations that CIs conduct are referred to the OI by the [Agency's] Allegations Review Board (ARB)[,]" which consists of a chairman, an office allegation coordinator, and one or more additional individuals within the appropriate office or region. *Id.* at 3. The RD also determined that a representative of the Agency's Office of General Counsel (OGC) or regional counsel must either attend ARB meetings, or review decisions made by the ARB, when allegations of suspected wrongdoing are discussed. *Id.* According to the RD, in cases involving suspected wrongdoing, "a representative from OI also attends ARB meetings for consultation and to provide information developed during any preliminary investigation conducted by the OI." *Id.* In addition, the RD determined that the ARB decides whether an allegation should be referred to the OI for investigation, or should be addressed in some other manner. *Id.* In this regard, the RD found that if the ARB refers an allegation to the OI, then the ARB issues a draft notice of investigation that specifies the legal and regulatory requirements that may have been breached. *Id.*

Further, the RD determined that once the ARB refers the investigation to the OI, a CI investigates the alleged violations specified in the notice. *Id.* The RD also determined that CIs exercise "a great deal of independence" in how they conduct their investigations, including obtaining and discussing "safeguards information"[4] if they find that they need to do so. *Id.* at 4. Additionally, the RD found that if a CI uncovers additional potential violations during an investigation, then the CI notifies the ARB, which then determines whether to expand the scope of the investigation. *Id.* at 3-4. Moreover, the RD found that during the investigation, if the OI uncovers potentially safety-significant issues that are not related to wrongdoing, then the OI forwards this information to the Agency's technical staff for appropriate action. *Id.* at 3.

The RD found that after the investigation is complete, the CI prepares a report of investigation (ROI) that includes a summary and analysis of the evidence, as well as the CI's opinion as to whether a willful or deliberate wrongful act was committed. *Id.* at 4. The RD also found that CIs' investigative reports are reviewed by their field office directors (FODs), and if the CI concludes that an action was deliberate or willful, then the matter is referred to the Department of Justice (DoJ) to determine whether to prosecute. *Id.* Further, the RD determined that in cases where DoJ declines to prosecute a deliberate or willful violation, or when the CI concludes that the action was not deliberate or willful, the matter is referred to the Agency's Office of Enforcement (OE), which convenes a panel -- including representatives from the Agency's OGC, regional offices, and technical staff -- to determine the appropriate administrative action. *Id.*

Based on these findings, the RD found that the CIs are engaged in investigative work concerning national security, specifically, the protection and preservation of the United States' "critical infrastructure." *Id.* at 15.

The RD found that the CIs' investigative work does not directly affect national security. *Id.* at 14. In this regard, the RD stated that CIs are not personally and directly responsible for the safety and security of Agency-licensed facilities. *Id.* at 15. In addition, the RD stated that there are "several intervening steps, both before and after," CIs become involved in conducting investigations. *Id.* Specifically, the RD found that normally, the ARB refers the investigation to the OI and determines the scope of the investigation by issuance of the draft notice of violation. *Id.* The RD also stated that, although the OI may initiate investigations, it does so "rarely." *Id.* at 3. Further, the RD found that at the end of an investigation, the CI's ROI is subject to review by the FOD and then, upon referral, is subject to further review and determination by either DoJ (for criminal prosecution consideration) or the OE (for decision on the appropriate administrative action). *Id.* at 15. Accordingly, the RD declined to exclude the CIs from the unit based on their investigative work. *Id.* at 15-16.

[4] Safeguards information is defined and discussed further below.

In addition, the RD found that the twelve CIs at issue in the application have never used or accessed classified information, and he declined to exclude them from the unit on that ground. *Id.* at 13-14. With regard to safeguards information, the RD found that several of the CIs do not have regular use of and/or access to that information, and that although they may obtain it if necessary during their investigations, the OI has a policy that they should do so only if necessary. *Id.* at 6. As for the CIs that have regular use of, or access to, safeguards information, the RD stated that the Authority examines the use of and/or access to "*classified* information[,]" and that "[i]t is undisputed that safeguards information is not classified information." *Id.* at 13 (citing *U.S. DoJ, Wash., D.C.*, 62 FLRA 286, 292-93 (2007) (Chairman Cabaniss concurring in part & dissenting in part) (*DoJ*)). Accordingly, the RD declined to exclude these employees from the unit on that basis. *Id.* at 15-16.

With regard to intelligence and counterintelligence work, the RD found that CIs perform duties as Federal Security Coordinators (Coordinators), in which capacity they exchange contact information with local, state, and federal law enforcement personnel stationed near nuclear power plants in order to enable the Agency to contact those personnel quickly in the event of an emergency or threat event at a plant. *Id.* at 4-5. In addition, the RD determined that CIs occasionally assist, and coordinate investigations with, law enforcement personnel from state, local, and other federal agencies. *Id.* at 5. Further, the RD found that some CIs participate in groups established to share law enforcement and intelligence information, including the Federal Bureau of Investigation's (FBI's) Joint Terrorist Task Force (JTTF), the FBI's Counterintelligence group, the Department of Homeland Security's Fusion Centers, and the United States Attorneys' Anti-Terrorism Advisory Council (ATAC). *Id.* The RD additionally determined that, during meetings of those groups, discussions can include classified information and "law enforcement sensitive information." *Id.*

The RD declined to find that the foregoing duties constitute "intelligence" or "counterintelligence" work within the meaning of § 7112(b)(6). *Id.* at 15. Finding that the Authority previously had not defined those terms, the RD applied dictionary definitions, *id.* at 11, and found that the CIs do not: (1) gather information concerning an enemy or possible enemy or a possible theater of operations; or (2) block an enemy's sources of information by concealment, camouflage, censorship, and other measures, to deceive the enemy by ruses and misinformation, to prevent sabotage, and to gather political and military information, *id.* at 15. Thus, the RD declined to exclude the CIs from the unit on this basis. *Id.*

In sum, the RD concluded that the CIs at issue: (1) perform investigative work that concerns, but does not directly affect, national security; (2) do not have regular use of, or access to, classified information; (3) should not be excluded from the unit on the basis of any access to safeguards information; and (4) do not perform intelligence or counterintelligence work. Accordingly, he declined to exclude them from the unit.

III. Positions of the Parties

A. Agency's Application

The Agency argues that the RD committed clear and prejudicial errors concerning substantial factual matters in finding that the CIs' investigative work does not directly affect national security.

To begin, according to the Agency, the RD "effectively diminished the role [of] OI representatives" in connection with their relationship to ARBs. Application at 28. Specifically, the Agency claims that, by characterizing OI representatives' participation in ARB meetings as "consultation," the RD "did not acknowledge that [they] provide valuable input . . . and are required participants" in those meetings, and did not acknowledge that they are an "integral component of the ARB and determining the case's initiation." *Id.* at 29. In addition, according to the Agency, the OI representative makes the final determination as to whether an allegation warrants an OI investigation, which the Agency claims supports its position that CIs' investigative work directly affects national security. *Id.* The Agency also asserts that OI may self-initiate investigations outside of the normal ARB process. *Id.*

In addition, the Agency asserts that the RD "incorrectly diminishe[d] the independent nature of the CI position," *id.* at 33, and "inaccurately describe[d] the process by which . . . [ROIs] lead[] to . . . enforcement action[s,]" *id.* at 32. In this connection, the Agency claims that, in stating that ROIs are subject to further review and determination, the RD: (1) ignored the fact that ROIs are not transmitted to DoJ and, instead, a separate investigative summary is sent to them, often before an ROI is completed, *id.*; and (2) "exaggerate[d]" the degree to which ROIs are subject to further review and determination by the FOD and OE, because, "[a]s with every government office, employees have varying levels of oversight and independence[,]" *id.* at 33, and although an Agency enforcement panel determines the appropriate action once an ROI is submitted, "CIs do not change or modify their conclusions regarding violations" when Agency offices disagree, *id.*

The Agency also contends that the RD failed to apply established law in finding that the CIs' investigative duties do not directly affect national security. *Id.* at 34. In this connection, the Agency claims that the RD based this finding on the "factual inaccuracies" alleged above. *Id.*

Further, apart from the foregoing investigative duties, the Agency argues that the RD committed clear and prejudicial errors concerning substantial factual matters because he "minimized the CIs' authority to access and use classified and safeguards information." *Id.* at 29. In this connection, the Agency asserts that CIs "may need to access" the information at any time, and that they have the requisite security clearance to do so. *Id.* In addition, the Agency challenges the RD's statement that CIs access safeguards information only if they have a need to know. According to the Agency, that statement inaccurately portrays CIs as "uniquely limited" in access to the information, when, in fact, it is a "fundamental security principle" that is not unique to OI. *Id.* at 30.

The Agency also challenges the RD's findings regarding classified information on the ground that he allegedly failed to apply established law. In this regard, according to the Agency, the RD acted contrary to Authority precedent because he "measure[d] the amount of time [that] a CI has actually used classified information . . . to determine bargaining unit status[,]" rather than recognizing that CIs may need to access classified information during the course of their duties. *Id.* at 36. For support, the Agency cites: *Social Security Administration, Baltimore, Maryland*, 59 FLRA 137, 146 (2003) (Chairman Cabaniss concurring and then-Member Pope concurring in part and dissenting in part) (*SSA*); and *United States Department of the Army, Corps of Engineers, United States Army Engineer Research Development Center, Vicksburg, Mississippi*, 57 FLRA 834, 837 (2001) (*Corps of Eng'rs*). *See* Application at 34 & 36. The Agency further claims, in this regard, that the RD's decision is "arbitrary" because "[t]he only difference between the employees the RD included and excluded . . . is that some of the CIs, simply by chance, were assigned specific investigations" that required them to use classified information. *Id.* at 36.

Moreover, the Agency contends that there is an absence of precedent regarding the meaning of "intelligence and counterintelligence" work under § 7112(b)(6). *Id.* at 26. According to the Agency, CIs perform liaison duties and coordinate with other federal, state, and local law enforcement and regulatory agencies "in an effort to share intelligence and counterintelligence information." *Id.* at 27. In addition, the Agency claims that, through meetings with JTTF, ATAC, and at Fusion Centers, during threat briefings, and in working with law enforcement and other agencies during the course of their investigations and assists to staff, CIs are engaged in intelligence and counterintelligence work that directly affects national security. *Id.*

Finally, the Agency argues that there is an absence of precedent regarding "the appropriate treatment of safeguards information in the context of [§] 7112(b)(6)," and that the Authority should treat safeguards information in the same manner as it treats classified information. *Id.* at 23. In this regard, the Agency asserts that much safeguards information cannot be "classified" information because it is owned by, produced by or for, or under the control of private industry, rather than the United States government. *Id.* at 24. Nevertheless, the Agency asserts that various statutes, Executive Orders, and Presidential Directives demonstrate that the nation's "critical infrastructure" includes the "[s]tructures and activities [that] are the subject of safeguarded material." *Id.* at 26. Accordingly, the Agency argues that the Authority should find that the regular use of, or access to, safeguards information directly affects national security under § 7112(b)(6), and exclude the CIs on this basis. *Id.* The Agency also argues that the RD "mischaracterized" the Agency's position as stating that safeguards information is "the equivalent" of classified information, *id.* at 30, which resulted in the RD "ignor[ing]" the Agency's legal arguments that 42 U.S.C. § 2167 (§ 2167) and the Agency's regulations demonstrate that, by definition, the unauthorized disclosure of safeguards information would have a direct effect on national security, *id.* at 31.[5]

B. Union's Opposition

The Union argues that the RD did not err by finding that the CIs' investigative work does not directly affect national security. Opp'n at 26. As for the Agency's claims regarding the OI's role during ARB meetings, the Union argues that: (1) the Agency's claim is not based on the actual duties of the CIs at issue in this case, because FODs, rather than CIs, usually serve as the OI representatives at the meetings; and (2) regardless of the CI's role in those meetings, that does not change the fact that there are several intervening steps before and after a CI is involved in a case. *Id.* at 28.

In addition, the Union contends that the RD did not err by focusing on actual, rather than potential, use and access to classified and safeguards information. *Id.* at 29-30. With regard to intelligence and counterintelligence work, the Union argues that CIs do not engage in such work. *Id.* at 23-26.

[5] The pertinent wording of § 2167 is set forth below.

With regard to whether safeguards information should be treated similarly to classified information, the Union claims that there is not an absence of precedent on this issue. *Id.* at 14. Specifically, the Union asserts that for employees who do not access classified information, a finding that an employee engages in security work is based on whether the employee designs, analyzes, or monitors security systems and procedures. *Id.* (citing *DoJ*, 62 FLRA at 290). Even if there is an absence of precedent on this issue, the Union argues that nothing in the plain wording or legislative history of § 2167 indicates that safeguards information "constitutes, is the equivalent of, or is meant to be a substitute for classified information." *Id.* In this connection, the Union asserts that, unlike classified information, there is a presumption that safeguards information should be available to the public, as evidenced by § 2167, which requires the Agency, when designating information as safeguards information, to place the minimum restrictions necessary to protect the health and safety or the public or common defense and security (the minimum-restrictions requirement). *Id.* at 17. Further, the Union notes that, unlike classified information, safeguards information does not expressly relate to "national security," but protects a "broader set of interests[,]" specifically, "health and safety" and "the common defense and security." *Id.* at 20. Moreover, citing *SSA*, 59 FLRA 137, the Union argues that the Authority "seeks to prevent the *incapacity or destruction* of . . . systems and assets [that] would have a *debilitating impact* on" national security, while § 2167 applies a different standard. Opp'n at 21. Finally, the Union argues that the "reasonably expects" standard for withholding safeguards information under § 2167 (i.e., that unauthorized disclosure could reasonably be expected to have a significant adverse effect) should not be construed as being the equivalent of the "reasonably expects" standard set forth in Executive Orders regarding classified information (i.e., that unauthorized disclosure could reasonably be expected to cause at least identifiable damage to the national security), because the legislative history of § 2167 indicates that the wording in § 2167 was "arrived at independently of the classified information standard and not intended to be consistent with it." *Id.* at 20-22.

IV. Analysis and Conclusions

As the RD stated, under § 7112(b)(6), a bargaining unit is not appropriate if it includes "any employee engaged in intelligence, counterintelligence, investigative, or security work which directly affects national security[.]" 5 U.S.C. § 7112(b)(6). Consistent with this statutory wording, to determine whether an employee is excluded from a bargaining unit based on § 7112(b)(6), the Authority must consider whether the employee is: (1) engaged in intelligence, counterintelligence, investigative, or security work that (2) directly affects (3) national security. *Cf. U.S. Dep't of the Air Force, Davis-Monthan Air Force Base, Ariz.*, 62 FLRA 332, 334 (2008) (Chairman Cabaniss concurring) (*Davis-Monthan*) (discussing security work).

The Agency argues that the RD failed to apply established law, and made clear and prejudicial errors regarding substantial factual matters, in connection with his findings that: (1) the CIs' investigative work does not directly affect national security; and (2) the CIs do not perform security work because they do not have regular use of, or access to, classified or safeguards information. In addition, the Agency argues that there is an absence of precedent with respect to the definitions of "intelligence" and "counterintelligence" within the meaning of -- and the appropriate treatment of safeguards information in the context of -- § 7112(b)(6). We address these arguments separately below.

A. The RD did not fail to apply established law, or make clear and prejudicial errors regarding substantial factual matters, in connection with his findings that the CIs' investigative work does not directly affect national security.

The RD found, and there is no dispute, that the CIs perform "investigative" work, and that this work involves "national security[,]" within the meaning of § 7112(b)(6). Rather, the Agency challenges only the RD's legal and factual findings regarding whether this investigative work "directly affects" national security.

The Authority has held that "directly affects" means "a straight bearing or unbroken connection that produces a material influence or alter[]ation." *U.S. Dep't of the Treasury, IRS*, 65 FLRA 687, 690 (2011) (Member Beck dissenting in part) (*IRS*). The Authority also has held that the plain terms of this definition -- that any bearing on national security must be "straight[,]" any connection must be "unbroken[,]" and any influence or alteration must be "material[]" -- make it clear that § 7112(b)(6) does not permit the exclusion of positions merely because they have *some* relationship to national security -- even "important national [security] interests." *Id.* Accordingly, applying this definition, the Authority has found that positions directly affect national security "only in limited circumstances." *Id.* For example, when there are "no intervening steps between the employees' failure" to satisfactorily perform their duties "and the potential effect [of that failure] on national security[,]" the Authority has found the requisite direct connection. *Id.* By contrast, where an employee's role in protecting national security is "limited," the Authority has not found the requisite direct connection.

Id. Similarly, where employees must "go through another individual" before their actions may impact national security, the Authority has declined to find a direct effect. *Id. See also U.S. Dep't of the Air Force, Tyndall Air Force Base, Tyndall AFB, Fla.*, 65 FLRA 610, 613 (2011) (*Tyndall*).

As an initial matter, the RD found, and there is no dispute, that CIs are not personally and directly responsible for the safety and security of Agency-licensed facilities. RD's Decision at 15. In addition, there is no dispute that the CIs are not engaged in designing or personally maintaining the security systems for, or security-related computer systems used in, Agency-licensed facilities. Thus, this case is distinguishable from Authority decisions where such employees' duties were found to directly affect national security. *See, e.g., U.S. Dep't of the Treasury, IRS*, 62 FLRA 298, 304 (2007) (Chairman Cabaniss concurring and then-Member Pope concurring) (among other things, employees granted and restricted access to agency facilities through issuance and deactivation of key cards, and determined the type and placement of security systems to be utilized in agency facilities); *DoJ*, 62 FLRA at 295-96 (employee was personally and directly responsible for maintaining the security of database used for many security-related purposes, including protecting the nation from terrorist attacks and storing military detainee information).

The Agency asserts that, in finding that the CIs' investigative work does not directly affect national security, the RD improperly "diminishe[d] the independent nature of the CI position," and states that CIs "do not change or modify their conclusions regarding violations" when Agency staff offices are not in agreement. Application at 33. In this connection, a relevant factor in assessing the "direct effects" requirement is whether employees' duties are "carried out in accordance with established procedures and provide[d] little opportunity for making choices[.]" *IRS*, 65 FLRA at 690. Consistent with this principle, the RD expressly acknowledged that CIs conduct their investigations with significant independence, and the Agency's assertion that CIs do not modify their conclusions merely because other staff offices disagree is a relevant consideration.

Nevertheless, the RD also found that the CIs do not have unfettered authority in conducting their investigations. In this regard, the RD found that *the ARB* -- not the CI -- "determines the scope of the investigation by issuance of the draft notice of violation." RD's Decision at 15 (emphasis added). In addition, the RD determined that if a CI uncovers additional, potential violations during the scope of the investigation, then the CI notifies the ARB, and *the ARB* -- not the CI -- "determines whether to expand the scope of the investigation." *Id.* at 4 (emphasis added). Thus, although CIs may exercise independence during the course of their investigations, the *scope* of those investigations is not entirely within their control. Put simply, their independence, while significant, is far from unlimited.

In addition, the RD found that there are several intervening steps, both before and after a CI's investigation, that limit the effect of the CIs' investigative duties on national security. In this regard, the RD found, and there is no dispute, that CIs' investigative reports are reviewed by their FODs.[6] *See id.* at 4. In addition, even after a CI completes his or her investigation, another entity or individual must actually take a prosecutorial or enforcement action before the CIs' investigative work can have an effect on national security. *See id.* at 15-16. As for the Agency's assertion that all government offices involve some layers of review, this does not change the facts that: (1) § 7112(b)(6) requires a "direct" effect on national security; and (2) the existence of intervening layers of review is a significant consideration in determining whether there is a direct effect. With regard to the Agency's claim that ROIs are not sent to DoJ for prosecutorial consideration -- and that only "a separate investigative summary" is sent to DoJ, Application at 32 -- the Agency does not explain why this demonstrates a direct effect on national security, particularly given that DoJ continues to serve as a separate, intervening layer between the CI's investigative work and any potential effect on national security.

Finally, with respect to ARB meetings, the Agency's arguments focus on the duties of a generic "OI representative," rather than the specific CIs at issue here. This focus is misplaced because in assessing bargaining unit status, the Authority focuses on "*only* . . . the duties of the position at issue." *Tyndall*, 65 FLRA at 613. In any event, even assuming that the CIs at issue

[6] As such, there is no basis for the dissent's assertion that, if a CI "wrongly conclude[s]" that no improprieties occurred, then no further action would be taken. Dissent at 21. In particular, the dissent cites no evidence that, upon review of an investigative report, an FOD cannot direct the CI to conduct additional investigative work.

perform the duties described in the application, that does not change the fact that there are several intervening steps before and after the performance of those duties that sever the link between those duties and any potential effect of those duties on national security.[7]

For the foregoing reasons, the Agency has not demonstrated that the CIs' investigative duties directly affect national security, and we do not exclude the CIs from the unit on that basis.

B. The RD did not fail to apply established law, or make clear and prejudicial errors regarding substantial factual matters, by focusing on CIs' actual, not potential, use of or access to classified and safeguards information.

As relevant here, an employee will be found to be engaged in "security work" within the meaning of § 7112(b)(6) if the employee's duties include "the regular use of, or access to, classified information." *Davis-Monthan*, 62 FLRA 332, 334. In assessing bargaining unit status, with certain exceptions not relevant here, the Authority focuses on the duties actually performed by the employee at the time of the hearing, rather than potential future duties. *SSA*, 59 FLRA 137, 142-43.

The Agency argues that CIs, due to their security clearances, could come into contact with safeguards and classified information at any time in the performance of their duties, and that it was "arbitrary" for the RD to include them in the unit while excluding CIs who, "simply by chance," have been assigned investigations that required them to access classified information. Application at 36. However, the Agency's arguments are misplaced because they focus on the CIs' potential duties in the future, rather than their actual duties at the time of the hearing, which is the relevant focus. *See SSA*, 59 FLRA at 142-43. Thus, the arguments do not provide a basis for reversing the RD. *See id.*

The Agency also challenges the RD's statement that OI policy restricts CIs to obtain safeguards information only when they need to do so, because the Agency claims that this principle does not apply only to CIs. There is no basis for finding that the RD relied on any perceived uniqueness of CIs in this connection, and, thus, the Agency's argument does not demonstrate that the RD made a clear and prejudicial error regarding a substantial factual matter.

With regard to the Agency's citations to *SSA*, 59 FLRA 137, and *Corps of Eng'rs*, 57 FLRA 834, those decisions held, respectively, that: (1) employees "do not lose their national security status simply because they are not engaged in matters related to national security *all* of the time," 59 FLRA at 146; and (2) the Authority does not require "any minimum amount of time" for access to classified material in order to find that an employee performs security work, 57 FLRA at 837. The Agency's reliance on these decisions is misplaced because, here, the RD did not find that the CIs are included in the unit merely because they do not have access to classified information "all of the time," 59 FLRA at 146 (emphasis omitted), or because they did not spend a "minimum amount of time" exposed to it, 57 FLRA at 837. Rather, the RD found that the CIs at issue in the application did not have *any* use of, or access to, classified information, despite the fact that at some point in the future their duties *could* require such use and/or access. Thus, the RD's decision is not contrary to *SSA* or *Corps of Eng'rs*.

For the foregoing reasons, the Agency has not demonstrated that the RD erred in finding that potential, future use of or access to safeguards and classified information is an insufficient basis for excluding the CIs from the unit.

C. There is an absence of precedent regarding the meaning of intelligence and counterintelligence work, but the Agency has not demonstrated that the RD erred in finding that the CIs do not perform such work.

As the RD found, no Authority precedent explains the meaning of the terms "intelligence" and "counterintelligence" under § 7112(b)(6). Thus, we find that there is an absence of precedent regarding the meaning of those terms.

Where the Statute does not define a pertinent term, the Authority has found it appropriate to consider dictionary definitions of the term. *AFGE, Local 1827*, 58 FLRA 344, 345-46 (2003) (Chairman Cabaniss concurring in part and Member Armendariz dissenting in part). The Statute does not define the terms "intelligence" and "counterintelligence." Accordingly,

[7] As the dissent does not reach the issue of exclusion of CIs on the basis of their access to safeguards information, Dissent at 22 n.*, the dissent's reliance on *Davis-Monthan*, 62 FLRA 332, which involved employees who had regular use of, and/or access to, classified information, is misplaced. Similarly, although it is undoubtedly true that, as the dissent states, CIs' investigative duties are "integral to the enforcement process as a whole," Dissent at 20, that is not the test for determining whether the CIs' *duties* directly affect national security. *Cf. IRS*, 65 FLRA at 690 ("[T]he mere fact that employees' work may have a relationship to important national interests is not sufficient to find a direct effect on national security.").

like the RD, we consider dictionary definitions of those terms.

In context, "intelligence" means "evaluated information concerning an enemy or possible enemy or a possible theater of operations and the conclusions drawn therefrom." *Webster's 3d New Int'l Dictionary* 1174 (2002) (*Webster's*). "[C]ounterintelligence" means "organized activity of an intelligence service designed to block an enemy's sources of information by concealment, camouflage, censorship, and other measures, to deceive the enemy by ruses and misinformation, to prevent sabotage, and to gather political and military information." *Id.* at 519.

The RD found that the record does not establish that any CIs are engaged in intelligence or counterintelligence work within these definitions. The Agency does not cite any record evidence indicating that the RD's finding is erroneous. In particular, the Agency does not show that any of the pertinent CIs are engaged in work that involves: (1) "evaluated information concerning an enemy or possible enemy or a possible theater of operations and the conclusions drawn therefrom," *Webster's* at 1174; or (2) "organized activity of an intelligence service designed to block an enemy's sources of information by concealment, camouflage, censorship, and other measures, to deceive the enemy by ruses and misinformation, to prevent sabotage, and to gather political and military information," *id.* at 519.[8] Further, the Agency provides no basis for finding that any intelligence or counterintelligence work that the CIs allegedly perform has a direct effect on national security, as required by § 7112(b)(6). Accordingly, we find no basis for reversing the RD and excluding the CIs from the unit on the ground that they are engaged in intelligence or counterintelligence work that directly affects national security.

D. There is an absence of precedent regarding the treatment of safeguards information in the context of § 7112(b)(6), and we find that the CIs who regularly use or access the safeguards information at issue here are engaged in security work that directly affects national security.

The Agency claims that there is an absence of precedent regarding the appropriate treatment of safeguards information in the context of § 7112(b)(6). The Union disputes this claim, asserting that *DoJ*, 62 FLRA 286, 290, establishes that, for employees who do not access classified information, the Authority assesses whether the employees design, analyze, or monitor security systems and procedures. However, *DoJ* did not establish an "either/or" standard. In addition, while the Authority previously has addressed access to certain types of non-classified information, the Authority previously has not been presented with, and thus has not addressed, access to the type of non-classified information -- safeguards information -- involved in this case. Accordingly, we conclude that there is an absence of precedent on whether regular access to safeguards information constitutes security work within the meaning of § 7112(b)(6), and we address that issue here.

The Authority has defined "security work" as "a task, duty, function, or activity related to securing, guarding, shielding, protecting, or preserving something." *U.S. DoD, Pentagon Force Prot. Agency, Wash., D.C.*, 62 FLRA 164, 171 (2007). In addition, as stated previously, the Authority has held that an employee will be found to be engaged in "security work" within the meaning of § 7112(b)(6) if the employee's duties include "the regular use of, or access to, classified information." *U.S. DoJ*, 52 FLRA 1093, 1103 (1997) (*Justice*). In *Justice*, the Authority rejected its previous holding in *Department of Energy, Oak Ridge Operations, Oak Ridge, Tennessee*, 4 FLRA 644, 655-56 (1980), that security work does "not include work involving mere access to and use of sensitive information and material." 52 FLRA at 1102. Instead, the Authority considered pertinent regulations and Executive Orders concerning classified material and concluded that the regular use of, or access to, such material is security work. *See id.* at 1102-03.

With regard to whether security work involves "national security," the Authority has held that the term "national security" includes:

> those sensitive activities of the government that are directly related to the protection and preservation of the military, economic, and productive

[8] We note that CI Teator testified that he was tasked at a counterintelligence working group with "obtaining information" and providing it to another federal agency for the conduct of their investigation into concerns regarding foreigners having access to special nuclear technology, *see* Tr. at 206-08, and CI Gonsoulin testified that he was assigned to JTTF to assist the FBI "in gathering information, intelligence that was coming in at that time," *id.* at 929. Even assuming that this testimony is sufficiently specific to demonstrate that these two CIs performed intelligence and/or counterintelligence work, CI Teator is not at issue here because the RD excluded him, and, for the reasons discussed further below, we find that CI Gonsoulin must be excluded on another ground. Accordingly, we do not address this testimony further.

> strength of the United States, including the security of the Government in domestic and foreign affairs, against or from espionage, sabotage, subversion, foreign aggression, and any other illegal acts which adversely affect the national defense.

Davis-Monthan, 62 FLRA 332, 335. This "entails, among other things, Government activities directly related to the protection of the economic and productive strength of the Nation, including the security of the Government from sabotage." *DoJ*, 62 FLRA 286, 291. The Authority has clarified that "such activities clearly include protecting the Nation's critical infrastructure, . . . as well as defending the Nation against terrorist activities." *Id.*

Applying the foregoing, the RD found, and there is no dispute, that the Agency's work concerns national security within the meaning of § 7112(b)(6). Specifically, the RD found that: (1) the Agency is responsible for the regulation of the United States' commercial nuclear power plants and use of nuclear materials, including the safe transport and disposal of nuclear materials and byproducts; (2) the United States' commercial nuclear power plants and the use of nuclear materials constitute a part of the Nation's critical infrastructure; and (3) any incapacity or destruction of these systems and assets would have a debilitating impact on security, the economy, public health and safety.

With regard to whether the CIs' *duties* -- specifically, the regular use of, or access to, safeguards information -- constitute security work that involves national security, we begin by considering the statutory and regulatory provisions pertaining to safeguards information. In this regard, § 2167, entitled "Safeguards information[,]" authorizes the Agency to

> prescribe such regulations, after notice and opportunity for public comment, or issue such orders, as necessary to prohibit the unauthorized disclosure of safeguards information which specifically identifies a licensee's or applicant's detailed--
>
> (1) control and accounting procedures or security measures (including security plans, procedures, and equipment) for the physical protection of special nuclear material . . . in quantities determined by the [Agency] to be significant to the public health and safety or the common defense and security;
>
> (2) security measures (including security plans, procedures, and equipment) for the physical protection of source material or byproduct material . . . in quantities determined by the [Agency] to be significant to the public health and safety or the common defense and security; or
>
> (3) security measures (including security plans, procedures, and equipment) for the physical protection of and the location of certain plant equipment vital to the safety or production or utilization facilities involving nuclear materials covered by paragraphs (1) and (2) if the unauthorized disclosure of such information could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of theft, diversion, or sabotage of such material or such facility.

42 U.S.C. § 2167(a).

Consistent with the regulatory authority set forth in § 2167(a), the Agency, in 10 C.F.R. § 73.2 (§ 73.2), has defined safeguards information, in pertinent part, as

> information not classified as National Security Information or Restricted Data which specifically identifies a licensee's or applicant's detailed control and accounting procedures for the physical protection of special nuclear material in quantities determined by the [Agency] through order or regulation to be significant to the public health and safety or the common defense and security; detailed security measures (including security plans, procedures, and equipment) for the physical protection of source, byproduct, or special nuclear material in quantities determined by the [Agency] through order or regulation to be significant to the public health and safety or the common defense and security; security measures for the physical protection of and location of certain plant equipment vital to the safety of production or utilization

> facilities; and any other information within the scope of [§ 2167], the unauthorized disclosure of which, as determined by the [Agency] through order or regulation, could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of sabotage or theft or diversion of source, byproduct, or special nuclear material.

10 C.F.R. § 73.2.

In addition, § 2167(a) provides that the Agency shall exercise its authority to prohibit the disclosure of safeguards information: (1) "so as to apply the minimum restrictions needed to protect the health and safety of the public or the common defense and security[;]" and (2) "upon a determination that the unauthorized disclosure of such information could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of theft, diversion, or sabotage of such material or such facility." 42 U.S.C. § 2167(a)(A), (B).

Further, § 2167(d) provides, in pertinent part, that, in connection with prohibiting the disclosure of safeguards information, the Agency shall submit a report to Congress that:

> (1) specifically identifies the type of information the [Agency] intends to protect from disclosure under the regulation or order;
>
> (2) specifically states the [Agency's] justification for determining that unauthorized disclosure of the information to be protected from disclosure under the regulation or order could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of theft, diversion, or sabotage of such material or such facility, as specified under [§ 2167(a)]; and
>
> (3) provides justification, including proposed alternative regulations or orders, that the regulation or order applies only the minimum restrictions needed to protect the health and safety of the public or the common defense and security.

42 U.S.C. § 2167(d).

Consistent with the foregoing, two things are clear. First, safeguards information includes, as relevant here, an Agency licensee's or applicant's security measures with respect to protecting nuclear materials and related equipment. Second, by designating the information at issue here as safeguards information and prohibiting its disclosure, the Agency has determined -- and justified its determination to Congress -- that the unauthorized disclosure of the information could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security, and that the minimum-restrictions requirement (i.e., the mandate that the Agency apply the minimum restrictions needed to protect public health and safety and the common defense and security) has been met.[9]

Here, the RD found, and there is no dispute, that the safeguards information that the CIs allegedly access involves the security plans of nuclear facilities. In addition, given the undisputed serious nature and scope of the potential effects that could result from sabotage of nuclear facilities, we find it reasonable to conclude that the unauthorized disclosure of security plans of nuclear facilities could have an adverse effect on the common defense and security. Although § 2167 uses the terms "common defense and security," rather than "national security," we find that nature of the safeguards information at issue here supports a conclusion that the information pertains to national security, and that the CIs' use of and/or access to it is "security work."

We note that § 73.2 defines safeguards information, in pertinent part, as "information *not* classified as National Security Information." (Emphasis added.) However, the Agency argues, and there is no dispute, that safeguards information is not classified as national security information because it is not information owned by, produced by or for, or under the control of the United States. *See* Application at 24. *See also* Executive Order (E.O.) 13,526 (stating that information may be classified only if, among other things, "the information is owned by, produced by or for, or is under the control of the United States Government"). The Authority has not previously held that information must be owned by, produced by or for, or under the control of the United States for that information to be related to national security. In this

[9] We note that there is no assertion that the Agency improperly categorized as safeguards information any of the information that CIs allegedly regularly use and/or access.

regard, as stated previously, national security work includes "activities . . . protecting the Nation's critical infrastructure, . . . as well as defending the Nation against terrorist activities." *DoJ*, 62 FLRA at 291. Further, E.O. 13,010, "Critical Infrastructure Protection," acknowledges that "many . . . critical infrastructures are owned and operated by the private sector." E.O. 13,010. Accordingly, the fact that the definition of safeguards information excludes "information . . . classified as National Security Information" merely reflects that safeguards information may not necessarily be owned by, produced by or for, or under the control of the United States and, as a result, cannot constitute classified information. It does not demonstrate that safeguards information does not concern national security, or that employees who regularly use or access safeguards information are not engaged in security work that relates to national security.

The Union argues that the plain wording and legislative history of § 2167 indicate that safeguards information was not meant to be the equivalent of, or a substitute for, classified information. However, nothing in the Statute or Authority precedent indicates that information must be the equivalent of, or substitute for, classified information in order to concern national security. Further, with regard to the Union's reliance on the minimum-restrictions requirement, that reliance is misplaced because, once information has been designated as safeguards -- as is the case with the information at issue here -- the Agency already has determined that the information meets that requirement. Moreover, the Union claims that § 2167 requires a different impact ("significant adverse effect") than the Authority requires -- specifically, "incapacity or destruction of systems that have debilitating impact." Opp'n at 21. However, the wording set forth in *SSA*, 59 FLRA 137, is from the statute and Executive Order that were at issue in that decision; the Authority did not hold that information must meet that standard in order for the information to concern national security. Even if it did, then it is reasonable to conclude that, should there be an unauthorized disclosure of the security plans of nuclear facilities, this could result in incapacity or destruction of systems that have debilitating impact. Finally, the Union claims that the "reasonably expects" standard that applies to safeguards information (i.e., that unauthorized disclosure could reasonably be expected to have a significant adverse effect) should not be construed as being the equivalent of the "reasonably expects" standard that applies to classified information (i.e., that unauthorized disclosure could reasonably be expected to cause at least identifiable damage to the national security). Opp'n at 20-21. However, that claim ignores that, in designating the information at issue in this case as safeguards information, the Agency already has made a determination that the unauthorized disclosure of the information could "reasonably be expected" to adversely affect the common defense and security. 42 U.S.C. § 2167(a)(B).

For the foregoing reasons, we find that the regular use of and/or access to the safeguards information at issue here is "security work" that involves "national security" within the meaning of § 7112(b)(6). Accordingly, consistent with the requirements of § 7112(b)(6), we next address whether the regular use of and/or access to this information *directly* affects national security.

In the context of classified information, the Authority has found a direct effect where, "given the nature of" the information at issue, "it is clear that there are no intervening steps between the employees' failure to prevent unauthorized disclosure of the . . . information that they use and/or access on a regular basis and the potential effect on national security should they fail to do so." *Davis-Monthan*, 62 FLRA at 335. No basis is argued for applying a different standard to safeguards information. Applying that standard here, given the nature of the safeguards information here -- the security plans of nuclear facilities -- and the fact that the Agency has determined (under statute and regulations) and justified to Congress that unauthorized disclosure "could reasonably be expected to have a significant adverse effect on . . . the common defense and security," *e.g.*, § 2167(d)(2), we find that there are no intervening steps between a CI's failure to prevent unauthorized disclosure of the information and the potential effect on national security. Accordingly, we find that, for employees who regularly use and/or access the safeguards information at issue here, they are engaged in national security work that directly affects national security.

The RD found that the following eight CIs have no, or only limited, use of or access to safeguards information: (1) Dvorak ("exposed to safeguards information on one occasion" in seven years, RD's Decision at 7); (2) Fahey (access on only "two occasions," *id.*); (3) Ferich (only "limited access" in six years, *id.*); (4) Hayden (only "limited exposure[,]" i.e., "once[,]" in seven years, *id.* at 8); (5) Janicki ("no access," *id.*); (6) Kryk (only "limited" access in twelve years, *id.*); (7) Richards ("has not used or had access," *id.* at 9); and (8) Young (has not "read or heard safeguards information," *id.* at 10). The Agency does not dispute these findings or allege that they support a conclusion that these eight CIs' actual use of, or access to, safeguards information is "regular."[10] Accordingly,

[10] As discussed previously, we have rejected the Agency's argument that the CIs should be excluded on the basis that they *could* use or access safeguards information in the course of their duties.

we find that these eight employees are not excluded from the unit on the basis of security work that directly affects national security.

However, the RD found that four CIs have access to, and/or use of, safeguards information that is sufficiently frequent to be characterized as "regular." Specifically, the RD found that: (1) Bigoness has had access "on several occasions" and is the custodian of the safe in which safeguards information is kept, *id.* at 7, which supports a conclusion that he has access on a continuous, or regular, basis; (2) Cabrelli has had access "several times," *id.*; (3) Gallagher has had access "several times[,]" *id.*; and (4) Gonsoulin "knows the combination to the safe" in which safeguards information is stored, *id.*, which supports a conclusion that he also has access on a continuous, or regular, basis.

Accordingly, consistent with the foregoing, we find that CIs Bigoness, Cabrelli, Gallagher, and Gonsoulin are engaged in security work that directly affects national security. Thus, we reverse the RD's Decision and Order in part on this basis and direct him to clarify the unit to exclude those four employees. We affirm the RD's Decision and Order in all other respects.

V. Order

The RD is directed to take appropriate action consistent with this decision.

Member Beck, Dissenting:

I disagree with my colleagues' conclusion that the Criminal Investigators' (CIs) investigative work does not directly affect national security.

As the Majority correctly notes, "'directly affects' means 'a straight bearing or unbroken connection that produces a material influence or alter[]ation.'" Maj. Op. at 8 (quoting *U.S. Dep't of the Treasury, IRS*, 65 FLRA 687, 690 (2011) (*IRS*) (Member Beck dissenting in part)) (alteration in original). Employees directly affect national security "when there are 'no intervening steps between the employees' failure' to satisfactorily perform their duties 'and the potential effect [of that failure] on national security.'" *Id.* at 9 (quoting *IRS*, 65 FLRA at 690). Applying this definition to the facts of this case, the investigative work performed by the CIs directly affects national security.

The CIs directly affect national security because they are personally and directly responsible for investigating alleged wrongdoing. *See U.S. Dep't of the Treasury, Internal Revenue Serv.*, 62 FLRA 298, 304 (2007) (*Treasury*) (Chairman Cabaniss and then-Member Pope concurring) (finding that the employees performed security work directly affecting national security because they were "personally and directly responsible" for designing, analyzing, and monitoring the security of the agency's facilities).[1] As the Majority acknowledges, the CIs exercise nearly complete control over the course of their investigations. Maj. Op. at 9. *See also* Tr. at 270; RD's Decision at 4 (finding that the "CIs act with a great deal of independence"). In doing so, the CIs independently develop an investigative plan, determine whom to interview, decide what evidence to gather or request, and conduct interviews and interrogations. Tr. at 87, 212-13, 270, 299.

[1] The Majority suggests that *Treasury* and *United States Department of Justice, Washington, D.C.*, 62 FLRA 286 (2007) (Chairman Cabaniss concurring in part and dissenting in part) are distinguishable because, in those cases, the duties for which the employees were "personally and directly responsible" involved security work. However, the Majority provides no reason why the analysis applied in those cases should not apply equally when an employee's investigative work is at issue. In fact, the Authority's test for whether an employee directly affects national security derives from security work cases. *See* Maj. Op. at 8-9 (citing *IRS*, 65 FLRA at 690 (setting forth "directly affects" test)). Further, the Majority itself relies upon security work cases in analyzing this matter. *See id.* at 10 (citing *U.S. Dep't of the Air Force, Tyndall Air Force Base, Tyndall AFB, Fla.*, 65 FLRA 610, 613 (2011) (discussing security work)).

Once an investigation is complete, the CIs write a report of investigation (ROI) analyzing the evidence they have gathered, determining whether a material false statement or regulatory violation occurred, and drawing a conclusion as to whether the action was willful or deliberate. *Id.* at 212-13. Once the CIs make a determination regarding willfulness, that conclusion is final. *Id.* at 553. Although field office directors (FODs) review the ROIs, they have little or no control over the investigation itself. *See, e.g., id.* at 347, 363, 548. In this regard, the FODs are limited to reviewing the evidence as provided to them by the CIs. *See id.* at 105 (Chief of the Office of Investigations (OI) testifying that CIs determine what evidence is necessary to make a conclusion and that an FOD would not know all of the evidence or information gathered by a CI).

That CIs are personally and directly responsible for their investigations is critical because their failure satisfactorily to perform their duties can directly affect national security. *See U.S. Dep't of Justice, Wash., D.C.*, 62 FLRA 286, 296 (2007) (*DoJ*) (Chairman Cabaniss concurring in part and dissenting in part) (finding that, because the employees were personally and directly responsible for the security of the agency's computer system, there were no intervening steps between the employees' failure to perform their duties and national security). In this regard, the CIs' investigations are integral to the enforcement process as a whole. These investigations are the only way by which action is taken against individuals who violate, willfully or not, the Agency's rules and regulations. Indeed, no enforcement action could be taken by either the Department of Justice (DoJ) or the Office of Enforcement (OE) without the information provided by the CIs. Therefore, the CIs' failure to satisfactorily perform their duties can result in unchecked wrongdoing, thereby compromising the Agency's security. *See Treasury*, 62 FLRA at 304 (finding a direct effect on national security because there was a direct connection between the employees' work and the agency's ability to perform its functions).

Such a conclusion is consistent with Authority precedent. For example, in *United States Department of the Air Force, Davis-Monthan Air Force Base, Arizona*, 62 FLRA 332 (2008) (*Davis-Monthan*) (Chairman Cabaniss concurring), the Authority found that the employees had access to classified information, such as troop deployments, travel of high level military officials, and mission data. *Id.* at 335. The Authority then determined that the employees' use of and access to that information had a direct effect on national security because "there [we]re no intervening steps between the employees' failure to prevent unauthorized disclosure of the classified information that they use[d] and/or access[ed] on a regular basis and the potential effect on national security should they fail to do so." *Id.*

Similarly, in *Treasury*, the Authority found that the employees had a direct effect on national security because "the work the Specialists perform[ed] and the security decisions they ma[de] [we]re critical to protecting the [a]gency's databases and physical facilities." 62 FLRA at 304. Specifically, the employees: "grant[ed] and restrict[ed] access to [a]gency facilities"; "periodically test[ed] the effectiveness of [the agency's] security measures"; and "detect[ed] security vulnerabilities at [a]gency facilities and ma[de] the necessary adjustments." *Id.*

The Majority determines that the CIs do not directly affect national security because there are "several intervening steps" – specifically, the Allegations Review Board (ARB) meetings and the DoJ/OE enforcement process – that, in the Majority's view, "sever the link between [the CIs'] duties and any potential effect of those duties on national security." Maj. Op. at 10. The Majority's analysis, however, fails to consider whether these supposedly intervening steps actually intervene between the employees' failure to perform their duties and the potential effect of that failure on national security. Applying this standard, I would find that neither the ARB meetings nor the involvement of DoJ/OE are "intervening steps."

With regard to the ARB meetings, these meetings occur before the CIs even begin their investigations. Tr. at 211-12. In this regard, the ARB issues a draft notice of investigation (notice) informing the CIs of what potential violation they are being assigned to investigate.[2] *Id.* at 228. The ARB has no involvement with the course of the investigation or with the conclusions reached by the CIs.[3] *See id.* at 40 (Chief of the Information Security Branch testifying that once an investigation is referred by the ARB, they are "out of the process"); *id.* at 81 (Chief of the OI testifying that "the Agency does not get involved once an OI investigation is initiated"). Accordingly, the ARB does not limit the CIs' discretion regarding these matters and, as a result, cannot prevent or mitigate any potential effect on national security that may result from the CIs' failure to perform their duties.

[2] The Majority suggests that the issuance of a notice determines the scope of a CI's investigation. Maj. Op at 9-10. However, the notice merely "specifies the legal and regulatory requirements that may have been breached." RD's Decision at 3. Further, as noted above and as the Majority itself concedes, the CIs "exercise independence during the course of their investigations." Maj. Op. at 10.

[3] Similar to the notice, the ARB can determine whether a new, potential violation discovered during a CI's investigation should be either investigated separately or included in the CI's current investigation. *See* RD's Decision at 4; Tr. at 227, 428.

Moreover, with regard to the DoJ/OE enforcement process, a case is referred to DoJ only when a CI has determined that a willful violation has occurred. *Id.* at 82-84. Further, in a case in which a CI has found no violation, the OE would have no basis to take any enforcement action. Thus, if a CI erroneously concludes either that there has been no violation or that no investigation is necessary, there can be no oversight by DoJ or the OE.

To illustrate, suppose a violator had stolen security plans for one of the Agency's nuclear power plants, and the ARB referred allegations about the theft to a CI to conduct an investigation. If the CI failed competently to perform his duties and wrongly concluded that the violator had engaged in no wrongdoing, the matter would not be referred to the DoJ or the OE for enforcement action.

As shown by this example, the ARB meetings and the DoJ/OE enforcement process cannot mitigate the failure of a CI to find, or thoroughly investigate, a potential violation. Therefore, these steps do not intervene between the CIs' *failure* to perform their duties and the potential effect of that failure on national security. *See Davis-Monthan*, 62 FLRA at 335 (finding a direct effect between a failure of employees to protect classified information and its potential effect on national security).

Accordingly, because the CIs are personally and directly responsible for their investigations, and because there are no intervening steps between their failure to satisfactorily perform their duties and the potential effect of that failure on national security, I would find that the CIs' investigative work directly affects national security. As a result, I would exclude all of the CIs from the bargaining unit.[4]

[4] Because I would exclude all of the CIs on this basis, I would find it unnecessary to address whether the CIs were engaged in intelligence or counterintelligence work or whether they may be excluded because of their handling of safeguards information.