



UNITED STATES OF AMERICA
BEFORE THE FEDERAL LABOR RELATIONS AUTHORITY
DALLAS REGION

DEPARTMENT OF JUSTICE
BUREAU OF PRISONS, FEDERAL CORRECTIONAL COMPLEX
BEAUMONT, TEXAS
(Agency)

and

AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL-CIO
(Union/Petitioner)

DA-RP-13-0011

DECISION AND ORDER

I. Statement of the Case

On May 15, 2013, the American Federation of Government Employees, AFL-CIO (AFGE, Petitioner, or Union) filed the petition in this proceeding with the Dallas Regional Office of the Federal Labor Relations Authority seeking a unit clarification to determine whether the Special Investigative Support Technician position GS-0303-08 (SIS Tech) at the Federal Correctional Complex in Beaumont, Texas (FCC Beaumont), currently encumbered by Michael Gardner, Brandi McBride, Jacoba Guzman, Gilbert Heritage, Christopher Barton, Lionel Becerra, Gary McCline, Stephen Smith, and Michelle McKinney, and the Intelligence Research Specialist position GS-0006-09 (IR Specialist), also at the FCC Beaumont and currently encumbered by Tanya Prejean and Robert Nylen, should be included in the existing certified nationwide consolidated bargaining unit of professional and non-professional employees represented by the Union. On August 8, 2013, a Notice of Hearing issued, setting an August 13, 2013 hearing date.

On March 31, 2006, in Case No. DA-RP-13-0011, a certification was issued by the Regional Director of the Federal Labor Relations Authority San Francisco Region certifying AFGE as the exclusive representative of the following bargaining unit of the following unit of employees:

Included: All professional and non-professional employees, including all Central Office employees, of the Bureau of Prisons and Federal Prison Industries, Inc., U. S. Department of Justice

Excluded: All Central Office temporary employees on appointments not to exceed 90 days; management, officials; supervisors; and employees described in 5 U.S.C. 7112(b)(2), (3), (4), (6), and (7).

The issues presented in this matter are as follows:

Whether the SIS Tech positions at the Federal Correctional Low (Low) and Medium (Medium) institutions encumbered by Gilbert Heritage, Stephen Smith, Christopher Barton, Michelle McKinney, Lionel Becerra, William Plake, Deborah Johnson, and Gary McCline should be excluded from the bargaining unit pursuant to Section 7112(b)(6) of the Statute because they are engaged in intelligence, counterintelligence, investigative, or security work which directly affects national security?

Whether the SIS Tech positions at the United States Penitentiary (USP or Penitentiary) encumbered by Michael Gardner, Brandi McBride, and Jacoba Guzman should be excluded from the bargaining unit pursuant to Section 7112(b)(6) and (7) of the Statute because they are engaged in intelligence, counterintelligence, investigative, or security work which directly affects national security or because they are primarily engaged in investigative or audit functions relating to the work of individuals employed by FCC Beaumont whose duties directly affect the internal security of the facility and they ensure those employees' duties are discharged honestly and with integrity?

Whether the IR Specialist position encumbered by Tanya Prejean and Robert Nylen should be excluded from the bargaining unit pursuant to Section 7112(b)(6) and (7) of the Statute because they are engaged in intelligence, counterintelligence, investigative, or security work which directly affects national security or because they are primarily engaged in investigative or audit functions relating to the work of individuals employed by FCC Beaumont whose duties directly affect the internal security of the facility and they ensure those employees' duties are discharged honestly and with integrity?

A Hearing Officer of the Authority held a hearing in this case on August 13, 2013, and parties filed briefs.¹ The evidence demonstrates that the SIS Techs and the IR Specialists are not primarily engaged in intelligence, counterintelligence, investigative, or security work which directly affects national security, nor are they primarily engaged in investigation or audit functions relating to the work of individuals whose duties directly affect the internal security of the agency to ensure that the duties are discharged with honesty and integrity. Accordingly, based on the evidence in the record, including all documentary and testimonial evidence submitted by both parties, I will clarify the Union's professional and non-professional bargaining unit to include the SIS Tech and IR Specialist positions.

II. Findings²

The Federal Bureau of Prisons was established in 1930 and its mission statement is:

¹ The Hearing Officer's rulings made at the hearing are free from prejudicial error and are affirmed.

² Consistent with the Authority's determination in *Dep't of Hous. & Urb. Dev., Wash., D.C.*, 35 FLRA 1249, 1256-1257 (1990), the eligibility determinations herein are based on testimony and other evidence establishing what an employee's actual specific duties were at the time of the hearing, rather than on speculation regarding what those duties might be in the future. While a position description may be useful in making a unit determination, it is not controlling.

To protect society by confining offenders in the controlled environments of prisons and community-based facilities that are safe, humane, cost-efficient and appropriately secure, and that provide work and other self-improvement opportunities to assist offenders in becoming law-abiding citizens.

The Federal Bureau of Prisons consists of 120 institutions, 6 regional offices, a Central Office (headquarters), 2 staff training centers, and 26 residential reentry management offices. The FCC Beaumont is located in Beaumont, Texas and is comprised of three distinct facilities: Federal Correctional Institution (FCI) Beaumont Low (Low), which houses low-security male inmates; the FCI Beaumont Medium (Medium), which houses medium security male inmates; and the United States Penitentiary Beaumont (USP or Penitentiary), which also houses medium security male inmates.

The SIS Office is responsible for conducting local investigations within the FCC Beaumont. In overseeing the SIS Office, Special Investigative Agents (SIAs) Joseph Ripka and Reshay Childress, along with SIS Lieutenants, supervise both the SIS Techs and IR Specialists. SIA Ripka supervises eight of the SIS Techs and one IR Specialist at both the Medium and Low facilities. SIA Childress supervises the four SIS Techs and the other IR Specialist at the Penitentiary.

The SIS Office monitors the Security Threat Groups (STGs), any unusual occurrences, criminal activity, and domestic or international terrorists. An STG is a domestic or national terrorist group, street gang, prison gang, or other disruptive group that has been identified as being a security threat in the Bureau of Prisons. Inmates in an STG may be classified as members, associates, or suspected as being a member or associate. It also monitors staff investigations and assists the Federal Bureau of Prisons' Office of Internal Affairs (OIA) with information on staff members for investigations. The SIAs and SIS Lieutenants both assign SIS Techs and IR Specialists staff and inmate investigations as part of their respective duties. The SIS Techs' and IR Specialists' responsibilities include monitoring phone calls of inmates, reviewing inmates' mail, emails, and other communications for any possible criminal activity. The primary difference between the two positions is that the IR Specialists experience greater levels of contact with outside law enforcement. When reporting the information to a superior, the chain of command is as follows: SIS Techs report to SIS Lieutenants, who report to the SIA; IR Specialists may report to either their SIS Lieutenant or to the SIA.

The Bureau of Prisons has several departments for classifying inmates in terrorist groups or other STGs. The Counterterrorism Unit (CTU), located in Martinsburg, West Virginia, monitors all domestic and international terrorists. It sets the monitoring guidelines and regulations for all facilities that house both domestic and international terrorists. The CTU has exclusive authority to decide whether an inmate is given a "terrorist" designation, it determines in which facility an inmate will serve his sentence, and it determines the level of monitoring for each inmate given a "terrorist" designation. "Monitoring" includes accessing phone calls, mail, and any electronic communications. The CTU also has access to the SIS Office's phone records, and uses the phone records and other monitoring to forecast trends within the FCC Beaumont.

The Sacramento Intelligence Unit (SIU) monitors gang-related activity or STGs within the Federal prison system. It classifies recently sentenced inmates as STG before they are transferred to federal

facilities and validates the inmates once they are identified as being a part of an STG. The SIU also determines what designation, within the STG classification, each inmate is given within the system. The Joint Terrorism Task Force (JTTF) is a group of multiple agency personnel that share information about local incidents within the law enforcement community. It hosts monthly meetings about potential national and international threats along with general information about current international events. The SIS Office is permitted to attend these meetings, but the level of information an employee may receive at these meetings is dependent on a security clearance.

A. SIS Technicians

The SIS Techs at FCC Beaumont serve as assistants to the SIAs. The SIS Techs' first-level supervisors are the SIS Lieutenants, who then report to the SIA or the Captain. Along with all other correctional institution employees, SIS Techs are charged with the responsibility of maintaining security of the institution. Their correctional responsibilities take precedence over all other duties required by their position and are performed on a regular and recurring basis. The SIS Techs primarily engage in research activities, which include the retrieval, review, and processing of medical documentation, central file documentation, monitoring videos, and monitoring inmate mail, email, and phone calls. They conduct search and retrieval of computerized monitoring operations to monitor inmates for suspicious activity. SIS Techs may also work in conjunction with SIAs in the investigation of alleged inmate or staff misconduct.

Unlike a correctional officer assigned to a post in a housing unit, the SIS Techs have no inmates assigned to them for custodial purposes. Rather, they monitor the general population for criminal activities or for ongoing terrorist or gang activity. Inmates normally arrive at the FCC Beaumont already "tagged" as being involved with an STG and all correctional officers must be aware of the designation. Each inmate is also given an opportunity for "self-admission" upon arrival if the inmate wishes to self-report his gang affiliation.

The SIS Techs must be aware of the inmates identified as STG, because they receive more vigorous monitoring than inmates with no group affiliation. At the time of the hearing, the Penitentiary was housing one domestic and two international terrorists. SIA Ripka testified that in terms of coming into contact with information on an inmate's STG activities, there is no difference between the correctional officers in the housing unit who have 100% access to the inmate and the SIS Techs who come into contact only when they are monitoring the inmate. That is, a correctional officer working a post in a housing unit, simply by overhearing a conversation or telephone call of an inmate, can come into contact with the same type of information that the SIS Techs may come across while monitoring that inmates phone calls, mail, or email.

The monitoring duties in which each SIS Tech engages vary by inmate and by SIS Tech. Because there are automatic placement criteria for inmates with certain offenses, monitoring requirements are in place for each inmate before he enters the facility, such as whether the inmate is on the required mail monitoring list. SIS Techs generate a weekly list of random inmates to be tested by a Urine Analysis (UA) Officer, who works with the SIS Office to help test inmates for controlled substances. Breathalyzer tests are performed on inmates monthly, but the SIS Techs also generate for the correctional staff a list of inmates who need more frequent testing.

SIS Techs conduct interviews for threat assessments and write memos about the interviews. These

interviews are discussions with inmates about their status. Upon request from supervisors, SIS Techs may respond to subpoena requests from outside law enforcement agencies, such as the Federal Bureau of Investigations or the Secret Service.

Every staff member, regardless of job position, is obligated to report any wrongdoing they witness other staff members committing. If, when reviewing video footage, an SIS Tech sees a staff member committing misconduct, the video must be put onto a CD to be reviewed by an SIA or other supervisor. The SIS Tech must also write a memo stating the facts of what was seen, but only the SIA or other supervisor determines whether misconduct has occurred and whether to make a referral to the Warden for further investigation, who would then decide whether to forward the matter to OIA or OIG. The SIS Tech may perform some cursory background search functions, such as looking up information on Lexis-Nexis, but may only do so with a supervisor's permission. They do not have the power to interview a staff member before providing the information to the SIA, nor do they have the power to request an alert on the staff member. SIS Techs may work alongside the SIAs who primarily investigate staff, but that task is limited to monitoring or copying telephone calls, mail, and email onto a CD.

i. SIS Technician Jacoba Guzman

Jacoba Guzman is an SIS Tech who had worked in the Penitentiary for two years at the time of the hearing. She is responsible for monitoring inmates' emails, recordings of inmates' phone calls, and inmates' outgoing mail. She frequently reviews written correspondence and telephone calls in Spanish. She also collects inmates' outgoing legal mail during the lunch hour. Legal mail is sealed when she receives it and each piece of legal mail is logged. She has neither intercepted any phone calls nor read any inmate mail that posed a threat to national security, and she has never had to pass any information she has discovered to either SIU or CTU.

Guzman's job duties, by necessity, have her interacting with inmates classified as STG. She assists in new inmate intake by taking pictures of the inmates and collecting their self-admission forms. The same intake procedure is followed regardless of whether the inmate has been classified as part of an STG. She also reviews and signs medical transfer paperwork noting STG status if an STG inmate needs hospital care. The SIS Office keeps bulletins from SIU and CTU to keep abreast of terrorism activities outside of the FCC Beaumont. Although SIS Techs are invited to attend meetings with the JTTF, Guzman rarely goes to the meetings. Guzman has not attended any meetings with the Warden and the SIA regarding terrorist inmates.

Guzman's job duties also include some security functions. She assists in responding to body alarms in the facility and with crime scene investigations. These tasks are only performed when there are incidents inside the institution. No crime scene investigation on which she has assisted has resulted in a staff investigation.

Guzman has assisted the SIA on employee investigations, but only when directed to do so by a supervisor. She does not have independent discretion to expand the scope of an employee investigation. While she has participated in interviewing staff members, lieutenants principally interview the staff members directly. She has never reviewed staff phone records or mail as part of an investigation and she has never testified in court about a staff investigation. During her two years in the SIS unit, she has viewed video that was later used in staff investigations three times and no

new policy or procedure has resulted from these investigations. Guzman has never performed any type of staff member audits or investigations of audits. She estimates that 10% of her time is spent performing staff investigations, while approximately 90% of her time is spent investigating inmates.

Guzman's regular duties do not involve cases dealing with terrorism or espionage and she is not certified in counterterrorism. She has not encountered terroristic information while in her current position. If she were to encounter this information, it would be passed to the CTU because CTU employees are certified in determining whether or not material is terroristic in nature. It is not in Guzman's regular duties to engage in protecting or defending the nation's critical infrastructure such as roads, telephones, or electrical systems. Guzman does not have security clearance and has access to that which is considered confidential information, but not to classified information. Guzman does not maintain classified or top secret information as a regular part of her job duties, nor does she maintain a vault or top secret material. She is not involved in the operations of a communication system that is used to communicate classified or top secret material. While there is a system in place for destruction of records, Guzman does not have the independent discretion to decide to destroy records. Guzman must have supervisory approval to look at other sources of information needed in an investigation.

ii. SIS Tech Brandi McBride

Brandi McBride is an SIS Tech currently assigned to the Penitentiary. At the time of the hearing, she had worked for the Bureau of Prisons for twelve years and had been an SIS Tech for ten years. McBride's job duties include maintaining office records of activity in the prison, such as assaults and gang activity. She also updates inmates' records on their contraband activities. In addition to monitoring inmates' emails, written correspondence, and phone calls, McBride monitors the video surveillance system within the prison. This monitoring is performed through watching either a live video feed or a recorded video. Occasionally she will pull recorded footage of an inmate incident for future use by the U.S. Attorney's Office as evidence in a legal proceeding against the inmate. The scope of all of McBride's monitoring work is determined by her supervisor. As with the other SIS Techs, McBride's monitoring duties include monitoring inmates on the STG alert list, which encompasses a "disruptive group" classification. Her monitoring of disruptive group members is normally limited to noting who they are associating with and monitoring their telephone activity for information about narcotics. McBride cannot conduct UA or Breathalyzer tests on inmates, nor does she assist in the testing.

McBride has more experience monitoring terrorist-related inmate activities than gang-related activities; since she has worked for FCC Beaumont there have always been inmates that were classified as some kind of terrorist. Accordingly, she interacts with outside law enforcement agencies such as the Office of the Inspector general (OIG) or the FBI more frequently than the other SIS Techs at the Penitentiary. McBride is familiar with the SIU, but she has not dealt directly with that office during her time at the prison. When she encounters information she suspects might be terrorism-related through her monitoring, she reports it to the CTU for further investigation. Throughout a CTU investigation, she will work with the office to provide any additional information it requires. All information submitted to CTU or JTTF must be passed to these organizations with her supervisor's knowledge and approval.

McBride has completed an SIS Tech-specific counterterrorism training, which provided an

overview of the Bureau of Prisons' counterterrorism efforts. McBride attends the JTTF meeting at least once a month, but is only permitted to attend the portion that is open to agents without security clearance. She provides the information to the local JTTF when any new inmate classified by the CTU as an international or domestic terrorist enters the FCC Beaumont.

Occasionally, McBride will assist the OIA in a staff member investigation. After another SIS Tech has reported potential staff misconduct to the SIA and the SIA reports it to OIA, OIA may refer the case back to the institutional level for fact-finding. McBride has taken affidavits and submitted the reports back to the OIA in these fact-finding investigations. In her 10 years as an SIS Tech, the information she has provided to the OIA has been used in approximately two staff investigations and no new policy or procedure has resulted from these investigations. McBride has never performed any type of staff member audits or investigations of audits. She estimates that approximately 25% of her time is spent performing staff investigation duties.

McBride's regular duties do not involve cases dealing with terrorism or espionage and she is not certified in counterterrorism. She has not encountered terroristic information while in her current position. If she were to encounter this information, it would be passed to the CTU because CTU employees are certified in determining whether or not material is terroristic in nature. It is not in McBride's regular duties to engage in protecting or defending the nation's critical infrastructure such as roads, telephones, or electrical systems. McBride does not have security clearance and has access to that which is considered confidential information, but not to classified information. McBride does not maintain classified or top secret information as a regular part of her job duties, nor does she maintain a vault or top secret material. She is not involved in the operations of a communication system that is used to communicate classified or top secret material. While there is a system in place for destruction of records, McBride does not have the independent discretion to decide to destroy records. McBride must have supervisory approval to look at other sources of information needed in an investigation.

iii. SIS Technician Michael Gardner

Michael Gardner is an SIS Tech at the FCC Beaumont Penitentiary. He has worked at the FCC Beaumont for a total of fourteen years, and as of the time of the hearing, has held his current position for ten years. As with all SIS Techs, Gardner's job duties include monitoring the inmates' phone calls, mail, and emails. As part of these monitoring duties, he also performs additional monitoring procedures for STGs and other inmates with alert status, such as a more detailed review of the STG inmates' phone calls and emails, financial transactions, and other actions. Along with the other SIS Techs, Gardner is also responsible for receiving and logging legal mail from the inmates during the lunch hour. Gardner estimates that his time spent reviewing inmates' phone calls, mail, and emails is about 10% of his daily duties.

In addition to his monitoring duties, Gardner assists with inmate intake, substance testing, and occasional general security duty. As part of the intake process, he reviews inmate pre-sentence reports, conducts entrance interviews, and photographs the inmates. Upon request from a unit manager, he will assist with administering UA and Breathalyzer tests to inmates, but he neither administers the tests nor generates the list of inmates to be tested. Gardner is sometimes called upon to assume the security duties if a lieutenant is on leave. He has never testified in court as to any incident in the prison. Gardner estimates that his time spent performing these other assigned tasks

is approximately 20%.

Gardner has completed an SIS Tech-specific counterterrorism training with CTU. This training provided a procedure for dealing with inmates suspected of terrorism and for passing information to CTU for additional translation or monitoring. He has responded to subpoena requests from outside law enforcement agencies in the past, but this is not a routine activity for him. Gardner has attended JTTF meetings, but does so approximately once or twice per year.

Gardner does assist in staff investigations, but based on his testimony at the hearing, it is apparent that his duties are limited to monitoring information. When questioned by the Hearing Officer, he had some difficulty estimating the exact percentage of time he spends on staff investigations. He ultimately testified that 70% of his daily duties are spent reviewing video footage in order to substantiate inmate allegations of staff impropriety. These allegations are received by the SIS Office and he is often tasked to review this footage by his supervisor. A smaller percentage of his time is spent taking and reviewing phone calls and emails and taking statements from staff and witnesses. He does not have the independent discretion to determine whether a staff member has committed misconduct. No new policy or procedure has resulted from his investigations. Gardner has never performed any type of staff member audits or investigations of audits.

Gardner's regular duties do not involve cases dealing with terrorism or espionage and he is not certified in counterterrorism. He has not encountered terroristic information while in his current position. If he were to encounter this information, it would be passed to the CTU because CTU employees are certified in determining whether or not material is terroristic in nature. It is not in Gardner's regular duties to engage in protecting or defending the nation's critical infrastructure such as roads, telephones, or electrical systems. Gardner does not have security clearance and has access to that which is considered confidential information, but not to classified information. Gardner does not maintain classified or top secret information as a regular part of his job duties, nor does he maintain a vault or top secret material. He is not involved in the operations of a communication system that is used to communicate classified or top secret material. While there is a system in place for destruction of records, Gardner does not have the independent discretion to decide to destroy records. Gardner must have supervisory approval to look at other sources of information needed in an investigation.

iv. SIS Technician Stephen Smith³

Stephen Smith is an SIS Tech at the FCC Beaumont Low, where he has worked since December 2012. Prior to that, he was an SIS Tech at the FCC Beaumont Medium from 2009 through 2012. As part of his duties, Smith performs internal inmate investigations, which occasionally includes STG members and international and domestic terrorists. For the inmates with a "terrorist" designation, Smith monitors incoming and outgoing telephone, email, and handwritten correspondences and the SIS Office forwards the correspondences to the inmate's CTU liaison if one is assigned, who makes the decision whether or not the SIS Office can release the messages. All correspondence to or from terrorists requiring translation are likewise forwarded to the CTU. For the remainder of the STGs, including terrorist inmates, he tracks, validates, and updates records for inmates coming into the

³ At the hearing, it was stipulated that SIS Tech Stephen Smith would provide representative testimony for all SIS Techs at the FCC Beaumont Low, including Gilbert Heritage, Christopher Barton, and Michelle McKinney.

facility.

Smith's regular duties do not involve cases dealing with terrorism or espionage and he is not certified in counterterrorism. He has not encountered terroristic information while in his current position. If he were to encounter this information, it would be passed to the CTU because CTU employees are certified in determining whether or not material is terroristic in nature. It is not in Smith's regular duties to engage in protecting or defending the nation's critical infrastructure such as roads, telephones, or electrical systems. Smith does not have security clearance and has access to that which is considered confidential information, but not to classified information. Smith does not maintain classified or top secret information as a regular part of his job duties, nor does he maintain a vault or top secret material. He is not involved in the operations of a communication system that is used to communicate classified or top secret material. While there is a system in place for destruction of records, Smith does not have the independent discretion to decide to destroy records. Smith must have supervisory approval to look at other sources of information needed in an investigation.

v. SIS Technician Lionel Becerra⁴

Lionel Becerra is an SIS Tech at the FCC Beaumont Medium Facility and at the time of the hearing, he had been in this position for approximately two years. His interactions with terrorist inmates are limited to monitoring their incoming and outgoing telephone calls, email, and handwritten correspondences. For all other STGs, including the terrorist group, he tracks, validates, and updates records for inmates coming into the facility. He will review inmates' pre-sentence reports, any media, and any self-admissions in order to gain an understanding as to the level of the security threat posed by the inmate.

Becerra's regular duties do not involve cases dealing with terrorism or espionage and he is not certified in counterterrorism. He has not encountered terroristic information while in his current position. If he were to encounter this information, it would be passed to the CTU because CTU employees are certified in determining whether or not material is terroristic in nature. It is not in Becerra's regular duties to engage in protecting or defending the nation's critical infrastructure such as roads, telephones, or electrical systems. Becerra does not have security clearance and has access to that which is considered confidential information, but not to classified information. Becerra does not maintain classified or top secret information as a regular part of his job duties, nor does he maintain a vault or top secret material. He is not involved in the operations of a communication system that is used to communicate classified or top secret material. While there is a system in place for destruction of records, Becerra does not have the independent discretion to decide to destroy records. Becerra must have supervisory approval to look at other sources of information needed in an investigation.

B. Intelligence Research Specialist

IR Specialists assist the SIA and the Lieutenants in conducting investigations through gathering investigative research and analyzing operational intelligence regarding the current activities of

⁴ At the hearing, it was stipulated that SIS Tech Lionel Becerra would provide representative testimony for all SIS Techs at the FCC Beaumont Medium, including Deborah Johnson, Gary McCline, and William Plake.

security threat groups, detainees, sentenced felons, Special Housing inmates and Special Confinement inmates. The IR Specialist also serves as FCC Beaumont's law enforcement liaison in referring criminal cases to other law enforcement agencies, such as the Federal Bureau of Investigation, United States Marshall Service, United States Secret Service, Alcohol Tobacco Firearms, Drug Enforcement Agency, among others, and presents cases to the United States Attorney's Office for possible prosecution. The incumbent prepares the case up to and including possible testimony before the Grand Jury and testimony during the criminal trial, and assists the U.S. Attorneys through the trial process. As with the SIS Tech, along with all other FCC Beaumont employees, the IR Specialist is charged with maintaining security at the institution. The staff's correctional responsibilities take precedence over all others required by this position and are performed on a regular and recurring basis.

IR Specialists assist SIAs in staff investigations. Their duties in staff investigations include pulling supporting documents, video, and phone calls to substantiate or discredit allegations of staff misconduct. The scope of the investigation is determined by the OIA, and the investigation is directed by the SIA. IR Specialists also join the SIA in monthly meetings to pass information to the OIG. They do not design the security systems or procedures used in their work.

i. Intelligence Research Specialist Tanya Prejean⁵

Tanya Prejean is an IR Specialist at FCC Beaumont. Prejean has been with the Bureau of Prisons for 17 years, 11 of which she has spent as an IR Specialist. Much of Prejean's functions are investigatory, and she estimates that approximately 85% of her time is spent investigating inmates, while the other 15% of her time is spent performing tasks as assigned by her SIA, which includes her staff investigation functions.

Prejean investigates disturbances within the institution and then supplies SIU, CTU, and the regional SIS with raw information in order for those units to determine how the information affects other institutions.

Prejean's other investigatory functions include monitoring inmate activities, STGs, and international terrorists through reviewing phone calls, emails, and using confidential informants (CIs). The CIs include other inmates and staff. While she does not always get her SIA's advance permission to follow any leads or to work directly with OIG, her SIA is eventually made aware that she is doing so. All information discovered in her investigations is reported to her SIA or other supervisor.

Prejean occasionally validates inmates during the intake process for association with any identified prison groups. This procedure involves interviewing the inmate, reviewing his pre-sentence report, and comparing his answers against the inmate's behavior and appearance, such as associating with known gang members or having gang-related tattoos. If an inmate meets certain criteria, she will upload the information for SIU determination as to whether or not the inmate should have STG status.

Many of Prejean's investigations relate to inmates possessing contraband, and many of these investigations start with inmates testing positive for narcotics. Occasionally, Prejean will also work

⁵ At the hearing, it was stipulated that Tanya Prejean would provide representative testimony for Robert Nylen.

with outside intelligence agencies who alert the SIS Office with information on STG inmates bringing contraband into the facility. She uses database research along with monitoring phone calls to determine how the contraband came into the inmate's possession.

Prejean gives informational briefings during the monthly staff meetings with the Warden. Her briefings include totals of Breathalyzer tests, the number of visitors scanned with drug substances, the total number of STGs, inmates who have tested positive for drugs, any weapons that were found, what assaults and fights took place in the prison, any incidents of staff uses of force, any inmates being watched, and any other unusual activity observed by staff in the institution. She does not attend JTTF meetings. She is certified to conduct trainings for narcotics identification kits but no longer actually conducts them.

Like the other employees in the SIS Office, Prejean works on staff investigations. Her involvement in staff investigations mainly stems from her inmate investigations. While she will participate in fact-finding, a process to ensure that staff did not commit misconduct, she is not responsible for taking affidavits from staff. Once an investigation has moved beyond fact-finding, she will continue to gather evidence to build a case against a staff member, but that information is passed through her SIA and up the chain of command for OIA or OIG to make the ultimate determination as to whether the staff member committed misconduct. She does not have the independent discretion to expand the scope of an investigation on a staff member. In Prejean's 11 years as an IR Specialist, she has assisted in approximately 5 staff investigations, including assisting OIG in one sting operation. No employee has been disciplined or removed, nor have any policies or procedures changed as a result of an investigation on which she has assisted. Prejean does not perform any type of staff audit or investigation of audits, except for a quarterly operational review to make sure that the entire SIS unit is in compliance with its expected duties and procedures. This review has no effect on performance appraisals.

Prejean's regular duties do not involve cases dealing with terrorism or espionage and she is not certified in counterterrorism. She has not encountered terroristic information while in her current position. If she were to encounter this information, it would be passed to the CTU because CTU employees are certified in determining whether or not material is terroristic in nature. It is not in Prejean's regular duties to engage in protecting or defending the nation's critical infrastructure such as roads, telephones, or electrical systems. Prejean does not have security clearance and has access to that which is considered confidential information, but not to classified information. Prejean does not maintain classified or top secret information as a regular part of her job duties, nor does she maintain a vault or top secret material. She is not involved in the operations of a communication system that is used to communicate classified or top secret material. While there is a system in place for destruction of records, Prejean does not have the independent discretion to decide to destroy records. Prejean must have supervisory approval to look at other sources of information needed in an investigation.

III. Analysis and Conclusions

The Authority is responsible for determining the appropriateness of units for labor organization representation under Section 7112 of the Statute. In Section 7112(b) of the Statute, Congress

precluded the Authority from finding appropriate any unit that included certain employees.⁶ Of relevance to this case, Section 7112(b)(6) of the Statute excludes from a bargaining unit any employee engaged in intelligence, counterintelligence, investigative, or security work which directly affects national security; while Section 7112(b)(7) of the Statute excludes from a bargaining unit any employee primarily engaged in investigation or audit functions relating to the work of individuals employed by an agency whose duties directly affect the internal security of the agency, but only if the functions are undertaken to ensure that the duties are discharged honestly and with integrity.

A. Section 7112(b)(6)

Under Section 7112(b)(6) of the Statute, Regional Directors must determine whether employees are (1) engaged in intelligence, counterintelligence, investigative, or security work that (2) directly affects (3) national security.⁷ Regarding the first prong of this test, the Authority has defined “security work” as “a task, duty, function or activity relating to securing, guarding, shielding, protecting or preserving something.”⁸ The Authority has held that this includes (1) the design, analysis or monitoring of security systems and procedures;⁹ and (2) work that involves the regular use of, or access to, classified information.¹⁰ The Authority has defined “intelligence” as “evaluated information concerning an enemy or possible enemy or a possible theater of operations and the conclusions drawn therefrom.”¹¹ “Counterintelligence” 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.”¹²

As to the second prong of the test, the Authority has found that “directly affects” means that there is “a straight bearing or unbroken connection that produces a material influence or alter[ation].”¹³ This definition means that Section 7112(b)(6) of the Statute does not permit the exclusion of positions merely because they have *some* relationship to national security—even “important national [security] interests.”¹⁴ This requirement is applied narrowly to implement Congress’s determination in Section 7101(a) of the Statute to “safeguard[] the public interest” through the institution of collective bargaining for federal employees.¹⁵ 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.”¹⁶

Conversely, the Authority has identified certain circumstances that make it less likely that an employee’s work directly affects national security. These include circumstances in which the

⁶ *U.S. Dep’t of Justice & Am. Fed’n of State, Cnty. & Mun. Employees, Local 3719, AFL-CIO*, 52 FLRA 1093 (1997).

⁷ *U.S. DOD, Pentagon Force Prot. Agency, Wash., D.C.*, 62 FLRA 164, 171 (2007) (*PFPA*).

⁸ *Dep’t of Energy, Oak Ridge Operation, Oak Ridge, Tenn.*, 4 FLRA 644, 655 (1980) (*Oak Ridge*).

⁹ *Id.*

¹⁰ *U.S. DOJ*, 52 FLRA 1093, 1102-03 (1997) (*DOJ*).

¹¹ *U.S. Nuclear Regulatory Comm’n*, 66 FLRA 311, 318 (2011) (*NRC*).

¹² *Id.*

¹³ *Oak Ridge*, 4 FLRA at 655.

¹⁴ *U.S. Dep’t of the Treasury, IRS*, 65 FLRA 687, 690 (2011).

¹⁵ *Id.* at 691.

¹⁶ *NRC*, 66 FLRA at 321 (quoting *Treasury*, 65 FLRA at 690).

employee's discretion is limited, such as employees carrying out duties in accordance with established procedures;¹⁷ circumstances in which the employee must "go through another individual" before his or her actions may impact national security;¹⁸ circumstances in which the employee performs numerous duties that do not involve national security;¹⁹ and circumstances in which individuals other than the employees at issue play an important role in the security of a facility.²⁰

Regarding the third prong of the test, the Authority has defined "national security" to "include only those sensitive activities of the government that are directly related to the protection and preservation of the military, economic, and productive strength of the United States, including the security of the [g]overnment in domestic and foreign affairs, against or from espionage, sabotage, subversion, foreign aggression, and any other illegal acts which adversely affect the national defense."²¹ This "entails, among other things, Government activities directly related to the protection and economic and productive strength of the Nation, including the security of the Government from sabotage."²² The Authority has further clarified this to include "such activities [as] protecting the Nation's critical infrastructure . . . as well as defending the Nation against terrorist activities."²³

Here, the evidence does not demonstrate that the SIS Tech and IR Specialist positions are engaged in intelligence, counterintelligence, investigative, or security work which directly affects national security. Applying the Authority test, there is no question that both positions involve investigatory work as well as a certain degree of security work. The employees in both positions investigate inmates, some of which are classified as "terrorist" or some other kind of STG. Employees in both positions are charged with maintaining security at the facility, as are all FCC Beaumont employees. The SIS Techs in particular monitor video security systems. Accordingly, I find that the SIS Techs and IR Specialists are engaged in investigative" and "security" work pursuant to Section 7112(b)(6) of the Statute and the first prong of the test is satisfied.

Even assuming that the SIS Techs' and IR Specialists' investigative and security work involves national security, the crux of the issue here is whether the SIS Techs' and IR Specialists' investigative and security work *directly affects* national security. While both positions' duties have some relationship to national security issues insofar as both positions have exposure to inmates labeled as international and domestic terrorists, the evidence does not support a finding of a direct effect of these duties on national security. While certain employees in either position may provide information on terrorists within the facility to either the SIU or the CTU, both positions have established protocols they must follow in their investigations. In fact, both SIS Techs and IR Specialists must go through several intervening levels of command before their investigations and security duties have any effect on national security. Neither position is permitted to identify whether or not material is terroristic in nature, and the employees must have SIA permission before they can

¹⁷ See, e.g., *U.S. Dep't of the Air Force, Tyndall Air Force Base, Tyndal AFB, Fla.*, 65 FLRA 610, 614 (2011) (*Tyndall*); *U.S. Dep't of Agric., Food Safety & Inspection Serv.*, 61 FLRA 397, 402-03 (2005) (*USDA*).

¹⁸ See, e.g., *USDA*, 61 FLRA at 402-03

¹⁹ *Treasury*, 65 FLRA at 692.

²⁰ See, e.g., *id.* at 691-92.

²¹ *Oak Ridge*, 4 FLRA at 655-66.

²² *NRC*, 66 FLRA at 319 (quoting *DOJ*, 52 FLRA at 1103).

²³ *Id.*

pass information to the CTU. Only CTU can decide whether material has any effect on national security. The employees do not perform criminal investigations on the terrorist inmates unless they happen to be assisting in a prosecution of an inmate for criminal activity. Their investigations are mostly limited to information-gathering. These limitations on their discretion break the “straight bearing or unbroken connection that produces a material influence or alter[ation]”²⁴ between the SIS Techs’ and IR Specialists’ duties and national security, and the second prong of the Authority test is not met.

Accordingly, considering the Authority’s narrow application of this exclusion,²⁵ I find that the SIS Techs’ and IR Specialists’ investigative and security work does not “directly affect” national security within the meaning of Section 7112(b)(6) of the Statute. Therefore, the SIS Techs and IR Specialists are not excluded from the bargaining unit of employees employed by the FCC Beaumont and represented by the Union under this section.

B. Section 7112(b)(7)

Section 7112(b)(7) of the Statute clearly excludes from bargaining units employees engaged in audit or investigative work whose functions are undertaken to ensure that the duties of the individual employees being audited or investigated are discharged “honestly and with integrity.” This exclusion is not limited to employees who perform investigations relating to “fraud, waste, and abuse,” but includes any audit or investigation that relates to employees’ “honesty” and “integrity.”²⁶

In *BOP Pine Knot*, the Authority analyzed an assertion that the investigation of inmates had the potential of becoming an investigation into staff misconduct because such an investigation inherently involves a review of whether staff could have prevented the incident and whether staff misconduct contributed to the incident and, thereby, increased the percentage of investigations related to staff.²⁷ The Authority noted, however, that Authority precedent demonstrates that the “potential for uncovering employee fraud, misuse of funds, or malfeasance” has been considered only in cases involving audits or investigations of agency programs or employees.²⁸ The Authority noted that “the word ‘primarily’ is capable of a range of meanings extending from ‘first’ or ‘chief’ to ‘substantially.’”²⁹ In holding that the employees at issue in *BOP Pine Knot* did not satisfy the “primarily engaged” requirement of Section 7112(b)(7) of the Statute, the Authority applied the standard in *Am. Fed’n of Gov’t Employees, Local 3529*, 57 FLRA 633 (2001) (*AFGE Local 3529*), in which the Authority held that employees are not excluded from a bargaining unit within the

²⁴ *Oak Ridge*, 4 FLRA at 655.

²⁵ *Treasury*, 65 FLRA at 690-91.

²⁶ *U. S. Department of Justice, Federal Bureau of Prisons, U. S. Penitentiary, Marion, Ill.*, 55 FLRA 1243 (2000) (The Authority instructed the Regional Director to “consider whether the Legal Assistant’s investigations of allegations that employees have used excessive force or have violated civil rights of inmates constitutes investigation of whether such employees have performed their duties honestly and with integrity.”).

²⁷ *United States Department of Justice, Federal Bureau of Prisons, U.S. Penitentiary, McCreary, Pine Knot, Ky.*, 63 FLRA 153 (2009) (*BOP Pine Knot*).

²⁸ *BOP Pine Knot*, 63 FLRA at 155 (citing *U.S. Dep’t of Labor, Office of the Inspector Gen., Region I, Boston, Mass.*, 7 FLRA 834, 835-36 (“potential” considered where auditors conducted audits of agency “programs and the employees who run these programs”); *SBA*, 34 FLRA 392, 401-02 (“potential” considered where auditors performed audits of agency “programs, contracts, operations, and program participants”)).

²⁹ *BOP Pine Knot*, 63 FLRA at 155 (citation omitted).

scope of 7112(b)(7) if “the preponderance” of their duties do not involve investigative functions set forth in that section of the Statute.³⁰ Despite spending the majority of their time on investigations of inmates that had the potential of developing into staff investigations, the Authority agreed with the Regional Director’s finding that employees at issue in *BOP Pine Knot* spent only 10-20% of their time on staff investigations.³¹

Applying the Authority’s “preponderance” standard to the present matter, the evidence does not support a finding that the SIS Techs and the IR Specialists are “primarily engaged” in investigations of staff to ensure that their duties are performed honestly and with integrity. While the SIS Techs and IR Specialists do perform staff investigations and many of those investigations are performed in response to inmate allegations of impropriety, the employees do not spend a preponderance of their time performing these investigations. Based on the hearing testimony, it is apparent that the SIS Techs and IR Specialists spend the majority of their days monitoring and/or investigating inmates. While these inmate investigations have the potential of leading to a staff investigation, each employee testified that they estimate they spend only 10-25% of their time actively involved with staff investigations. Because the standard for exclusion under 7112(b)(7) is 50% or more of an employee’s time spent on staff investigations, the employees at issue here fall short of this benchmark.

Accordingly, I conclude that the SIS Tech and IR Specialist positions are not excluded from the bargaining unit pursuant to Section 7112(b)(7) because while they do perform investigation or audit functions relating to the work of individuals employed by the agency whose duties directly affect the internal security of the agency and these functions are undertaken to ensure that the duties are discharged honestly and with integrity, the SIS Techs and IR Specialists are not primarily engaged in these investigations.

IV. Order

For the above reasons, an appropriate Clarification of Unit will be issued reflecting the position of SIS Technician, GS-0303-08, and the Investigative Research Specialist, GS-0006-09, is included in the following unit of employees represented by AFGE:

Included: All professional and non-professional employees, including all Central Office employees, of the Bureau of Prisons and Federal Prison Industries, Inc., U. S. Department of Justice


Excluded: All Central Office temporary employees on appointments not to exceed 90 days; management, officials; supervisors; and employees described in 5 U.S.C. 7112 (b)(2), (3), (4), (6), and (7).

³⁰ *Id.* at 155-56 (citing *AFGE Local 3529* at 638; *Obremski v. Office of Pers. Mgmt.*, 699 F.2d 1263, 1270 (D.C. Cir. 1983) (interpreting an OPM statute to find that an employee who spend thirty percent of his time doing work related to detention “would not be primarily engaged” in detention)).

³¹ *Id.* at 156.

V. Right to Seek Review

Under Section 7105(f) of the Statute and Section 2422.31(a) of the Authority's Regulations, a party may file an application for review with the Authority within sixty days of this Decision. The application for review must be filed with the Authority by **October 14, 2014**, and addressed to the Chief, Office of Case Intake and Publication, Federal Labor Relations Authority, Docket Room, Suite 201, 1400 K Street, NW, Washington, DC 20424-0001. The parties are encouraged to file an application for review electronically through the Authority's website, www.flra.gov.³²



James E. Petrucci
Regional Director, Dallas Region
Federal Labor Relations Authority

Dated: August 20, 2014

³² To file an application for review electronically, go to the Authority's website at www.flra.gov, select **eFile** under the **Filing a Case** tab and follow the instructions.

CERTIFICATE OF SERVICE

Case No. DA-RP-13-0011

I hereby certify that on August 20, 2014, I served the foregoing **Decision and Order**, issued by James E. Petrucci, upon the interested parties in this action by placing a true copy, postage prepaid, in the United States Post Office Mailbox at Dallas, Texas, addressed as follows:

Chief
Office of Case Intake and Publication
Federal Labor Relations Authority
Docket Room, Suite 201
1400 K Street, NW.
Washington, D.C. 20424-0001

Certified Mail No. 7013 2250 0001 8222 5451

Valerie J. Jackson
Labor Relations Specialist
LRO-South
346 Marine Forces Drive
Grand Prairie, TX 75051

Certified Mail No. 7013 2250 0001 8222 5468

Julia Altum
Attorney
AFGE, AFL-CIO
80 F Street, NW
Washington, DC 20001

Certified Mail No. 7013 2250 0001 8222 5475

Peter A. Sutton
Deputy General Counsel
Office of the General Counsel
Federal Labor Relations Authority
1400 K Street NW, Second Floor
Washington DC 20424-0001

