2011-02460-IQ-0112

Memorandum to the File
Case Closure

Alleged Ethical, Acquisition, and Information Security Violations; Misuse of Government Resources; and Prohibited Personnel Practices, VISN 5, Linthicum, MD
(2011-02460-IQ-0112)

The VA OIG Administrative Investigations Division investigated allegations that (b) (7)(C) for VISN 5, gave preferential treatment to a contractor employee and a contractor; misused Government resources to pay for training and travel for contractor employees; instructed contractor employees to perform tasks outside the scope of their contracts; gave personnel improper elevated access to VA information systems; and gave preferential treatment to an applicant. To assess these allegations, we interviewed the complainant, (b) (7)(C) (b) (7)(C) We also reviewed emails, contract records, contractor resumes, records for contractor training and travel, information system privilege documents, and personnel records, as well as applicable Federal laws and regulations and VA policies.

Federal law prohibits granting any preference or advantage to any employee or applicant for employment for the purpose of improving or injuring the prospects of any particular person for employment. 5 USC § 2302(b)(6). Federal regulations require that selection and advancement be determined solely on the basis of relative ability, knowledge, and skills, after fair and open competition. 5 CFR § 2301(b)(1).

Standards of Ethical Conduct for Employees of the Executive Branch require that employees act impartially and not give preferential treatment to any private organization or individual and that employees endeavor to avoid any actions creating an appearance that they are violating the law or these ethical standards. 5 CFR § 2635.101(b)(8) and (14). They also require that employees protect and conserve Federal property and not use such property or allow its use for other than authorized activities. Id., 2635.704. Federal acquisition regulations (FAR) require that Government business be conducted in a manner above reproach and with complete impartiality and preferential treatment for none. 48 CFR § 3.101-1.

VA policy states that logical access controls are employed to permit only authorized access to VA computer systems and restrict users to authorized transactions, functions, and information. These automated controls ensure that only authorized individuals gain access to information system resources; these individuals are assigned an appropriate level of privilege; and they are individually accountable for their actions. Access to system security files, system management/configuration files, and creation of shared drives and other protected files is limited to OI&T staff that requires this access in order to perform their duties. VA Handbook 6500, Paragraph C(2)(a) and (b).

Background:

(b) (7)(C) told us that she was the lead for (b) (7)(C) project initiated in late 2008 to create a computer database used for reporting and analysis for use by VISN 5 managers and analysts. The data stored in the warehouse is uploaded from operational computer systems, such as VA Medical Center systems, and used by managers and analysts to create reports, analyze trends, and perform other business functions. Contracting documents reflected that three IT companies, Hitachi Consulting, Key Logic Systems, and Black Hawk Consulting, worked under contract with VA for the project.

Alleged Preferential Treatment

In reference to the allegation that (b) (7)(C) gave preferential treatment to a contractor employee by allowing the employee to telework yet denied those privileges to another contractor employee, we found that each of the data warehouse contracts contained a clause stating, "contract staff will perform on-site with the VA staff at the VISN office in Linthicum, Maryland." (b) (7)(C) told us that, in the initial stages of the project, the former (b) (7)(C) did not want any contractor or VA employee to telework, because the project required close teamwork. She said that in the early stages of the project, she and (b) (7)(C) turned down a contractor employee's request to telework for extended periods, because the project was in its "infancy." She said that they did not feel comfortable allowing any of the team members teleworking. She also said that if any contractor employee asked to telework at that time, their request would have been denied.

(b) (7)(C) told us that as the project matured the project leaders began to feel more comfortable allowing team members to telework. She said that one contractor employee was prepared to leave the project, because he needed to move closer to his family in North Carolina to get care and medical attention for his ill child. She also said that she, the other project leaders, and Hitachi management agreed to ask the employee if he would be willing to continue on the project working remotely. The Hitachi employee agreed, and they did a contract modification to allow him to telework from his home in North Carolina. (b) (7)(C) said that a VA employee and another contractor employee involved in the project were also allowed to Telework.

(b) (7)(C) and the (b) (7)(C) told us that, in the early stages of the project, some contractor employees wanted to telework but were turned down, because (b) (7)(C) wanted all the team members to work together on-site. They said that the one Hitachi employee was allowed to telework when the project was at a more mature stage and telework became more feasible. The (b) (7)(C) (b) (7)(C) also told us that the Hitachi employee had a "life change" that required him to move to North Carolina and the project managers did not want to lose the Hitachi employee's knowledge and expertise, as well as the continuity he brought to the project. He said that since the Hitachi employee's tasks could be performed remotely, they decided to allow him to telework. (b) (7)(C) said that a Black Hawk

employee was also allowed to telework and that in both cases, they performed a contract modification to allow each contractor employee to telework.

Contract records reflected that the contracting officer signed a contract modification in September 2011 to allow an Hitachi employee to telework from Raleigh, NC, "on a case-by-case basis, with prior approval from the COTR" and "at no additional cost to the Government." Records also reflected that the contracting officer signed a similar contract modification in October 2011 to allow a Black Hawk employee to telework from McKinney, TX.

In reference to an allegation that (b) (7)(C) gave preferential treatment to Hitachi Consulting by allowing the company to assign an unqualified contractor employee to a particular tasking on the data warehouse project, (b) (7)(C) told us that she did not know anyone from Hitachi or anything about the company before they were awarded the contract. She said that all the contractor employees assigned to the project had the skills and qualifications required by their contracts and that she knew of no instance in which they accepted a Hitachi employee or any other contractor employee who did not have the required qualifications. She said that before the contractor employees were assigned to the project, they were interviewed by a panel of VA employees to determine whether they had the necessary IT skills and could work well in a team environment.

Three VA employees told us that, before accepting the Hitachi employee for the contract, (b) (7)(C) and other team members reviewed the employee's resume and interviewed the employee to determine whether he was qualified. (b) (7)(C) explained that when a contractor presented a candidate for the contract, he, (b) (7)(C) and one or two other people on the team reviewed the candidate's resume and interviewed him or her to determine whether the candidate had the necessary IT skills. He said that the panel also evaluated the candidates on their communications skills and their ability to understand program requirements. Further, he said that the decision to accept or reject a candidate was a consensus decision by the panel members and not just a decision by (b) (7)(C)

(b) (7)(C) told us that he was a member of the panel that interviewed the Hitachi employee in question and that the employee had the required qualifications for the identified task, which involved building and deploying reports. He said that the employee's resume reflected that the employee had training in SSRS and work experience using SSRS software to retrieve data and generate reports from a data warehouse, which showed that the employee was qualified for the SSRS task. He also said that the employee performed well on the task and his reports were "really good." He told us that he never saw (b) (7)(C) give Hitachi or its employees any preferential treatment. The (b) (7)(C) told us that he did not participate in the Hitachi employee's interview, but he said that he believed the employee was qualified. He said that the employee worked successfully on the project for a year before leaving to take another job.

Alleged Misuse of Government Resources

In reference to an allegation that (b) (7)(C) improperly paid for an Hitachi employee to attend a conference, (b) (7)(C) said that it was "second hand" information, and (b) (7)(C) could provide no date or location of the conference, what funds were used to pay for the travel, or the contractor employee's name. Further, (b) (7)(C) could not give us the names of the individuals who gave (b) (7)(C) this information. Since (b) (7)(C) did not provide sufficient information for us to investigate this allegation; we did not pursue it further.

Alleged Improper Contractor Employee Training

In reference to an allegation that (b) (7)(C) gave a Key Logic contractor employee on-the-job training in commercial software packages, to include SQL Server Reporting Services (SSRS), SharePoint, and PerformancePoint, (b) (7)(C) denied providing this type of training to a Key Logic contractor employee or any other contractor employee. (b) (7)(C) told us that the Key Logic employee was proficient in SharePoint and, in fact, trained VA personnel on this software. She said that contractor employees received some training when they came to work on the project, but this did not include training in commercial software. She also said that the contractor employees had to be oriented to the VHA and familiarized with VHA-specific systems, the location of data, and the plan for creating the data warehouse but that the contractor employees came to the project fully trained with the necessary IT skills for their tasks.

Two VA employees assigned to (b) (7)(C) told us that they never saw the Key Logic contractor employee or any other contractor employee receive on-the-job training in commercial software packages. (b) (7)(C) said that the Key Logic employee was an expert in SSRS and helped other team members with this software and that he was also proficient in SharePoint and PowerPoint. (b) (7)(C) (b) (7)(C) said that contractor employees received initial training on such topics as VA systems and processes, how to access VA information systems, VA electronic medical records, and VA health care processes, but not in commercial software packages. Another VA employee said that contractor employees often shared their expertise with other team members, to include VA and contractor employees, by demonstrating software "tricks." He considered this "information swapping" and not training.

In reference to (b) (7)(C) allegedly misusing Government funds to pay for a Key Logic contractor employee to attend Team Foundation Services (TFS) training in January 2011, email records reflected that (b) (7)(C) requested that the Key Logic employee attend advanced TFS training given by VA in January 2011. (b) (7)(C) told us that that there was no cost to the Government for tuition, since VA was already giving the training, but email records reflected that (b) (7)(C) proposed reimbursing the contractor for half the employee's travel expenses, since the training benefited both VA and the contractor. On March 19, 2011, the contracting officer signed a contract modification stating that the VA would reimburse Key Logic for one half of the contractor employee's travel costs.

(b) (7)(C) told us that she sent the Key Logic employee to the TFS training for the benefit of VA. She said that she chose the Key Logic employee to attend the training, as he was the team member most proficient in TFS software. She also said that once the Key Logic employee completed the training, he shared what he learned with other team members. (b) (7)(C) said that she believed it was appropriate for VA to pay for a contractor employee to attend training if such training was needed for the project and that she worked with the contracting officer to ensure that this was done "appropriately."

VA employees assigned (b) (7)(C) also told us that the Key Logic employee attended VA-sponsored TFS software training for the benefit of VA. (b) (7)(C) told us that the data warehouse team used TFS, but they wanted to use expanded TFS functionality and needed a "resource person" on the team who was knowledgeable in this expanded TFS function. (b) (7)(C) said that VA had an open slot tor TFS web applications training; they decided to send the Key Logic employee, since he was the team member with the most TFS experienced; and he would then function as the team's resource for TFS web applications. Another VA employee told us that the Key Logic employee was sent to the training, as he was already a TFS specialist and the team member most proficient in the software. He said that the employee learned about the advanced features, and when he returned from training, he taught other team members how to use those advanced features.

In reference to an allegation that (b) (7)(C) improperly allowed a Black Hawk employee to attend IT training intended for VA employees, (b) (7)(C) told us that in 2011 Black Hawk gave analysis service training to VA employees at its company in West Virginia and that the Black Hawk employee did not attend as a student but rather as a "teaching assistant" for the class, providing training to VA employees. He said that this was not a misuse of Government resources, as the contractor provided training to VA employees rather than receiving training at Government expense.

Alleged Improper Contracting

In reference to an allegation that (b) (7)(C) engaged in improper contracting when she allowed contractor employees to perform work outside the scope of their task orders, in a memorandum dated May 19, 2010, (b) (7)(C) responded to a VA employee's concerns that contractor employees performed work outside the scope of their task orders. In this memorandum, (b) (7)(C) said that, as COTR for the data warehouse contracts, she discussed the matter with the contracting officer and developed a solution to ensure the Statements of Work allowed the contractor employees to work at various tasks within the project.

(b) (7)(C) told us that when the VA employee brought this matter to her attention, she sought advice from the contracting officer and that the contracting officer told her that if a contractor employee had additional skill sets, it was permissible to allow the employee to use those skills to perform work outside the specific task for which the employee was hired, as long as it was within the (b) (7)(C) project. (b) (7)(C) said that the contracting officer also told her that, if she wanted to be covered, the contracting officer

would execute contract modifications to allow contractor employees to perform work outside their specific tasks. (b) (7)(C) said that she drafted contract modifications for each of the three contractors involved in the project and these contract modifications were approved and signed by the contracting officer.

(b) (7)(C) said that the contract modifications were for the benefit of VA; however, the contractor managers also had to approve and sign the contract modifications. (b) (7)(C) said that she did not hear any objections from any of the contractors or concerns of another contractor infringing on their tasks. (b) (7)(C) further said that the contractors did not lose any money, as the contractor employees were always busy, due to the immense amount of work to do on the project.

Contract records reflected that in July and August 2010, the contracting officer signed contract modifications for the three contractors, adding a requirement that the contractor employees "utilize their wide range of Business Intelligence skills in order to support the VISN 5 (b) (7)(C) project." These modifications were incorporated into the statements of work. (b) (7)(C) told us that she did not remember what led up to the contract modifications, but she said that she did not see any problem with the modifications. (b) (7)(C) also said that she did not hear any complaints from the contractors about employees working outside the scope of their task orders.

Alleged Violation of VA's Information Security Policy

In reference to an allegation that (b) (7)(C) directed the VISN 5 database administrator to grant VA employees and contractor employees elevated (programmer and/or system administrator) access to VA information systems, in violation of VA Handbook 6500, "Information Security Program," (b) (7)(C) told us that in late 2008, a VA employee assigned to the (b) (7)(C) project requested programmer access to the system. He said that he refused to give the employee this access, because he said that in granting such access to a non-OI&T employee would violate VA Handbook 6500, which states that "access to system security files, system management/configuration files, and creation of shared drives and other protected files is limited to OI&T staff that requires this access in order to perform their duties." He further said that when (b) (7)(C) asked him to give the VA employee programmer access to the system, he told her that it would be a violation of VA policy and that she would have to give him a written order to do so. He said that on February 24, 2009, (b) (7)(C) sent him an email directing him to grant programmer access to the VA employee. He told us that (b) (7)(C) also gave contractor employees and another VA employee elevated access to the data warehouse systems, which he considered violated VA policy.

(b) (7)(C) told us that it was proper for VA employees to have elevated access to the data warehouse system, because she said that they needed this access to do their jobs, which involved building data and creating reports using the data warehouse. She also said that they used their access to create "data queues, data marks, and reports," and that this access did not violate VA policy, since they were not accessing "the inner workings" of the servers or performing system administrator functions. She said that

these were handled by the database administrator and OI&T staff. (b) (7)(C) also said that contractor employees having elevated access to the data warehouse system did not violate VA policy, as contractor employees working under OI&T contracts were considered OI&T employees.

(b) (7)(C) told us that when the DBA brought this matter to his attention in early 2009, he did some research and consulted with the Regional Network Information Security Officer (ISO). He concluded that (b) (7)(C) had the authority to grant elevated access to non-OI&T personnel. (b) (7)(C) told us that his interpretation of the VA policy for granting elevated access was that the (b) (7)(C) was the "system owner" and had the authority to grant whatever access she deemed necessary to get the work done. He cited paragraph 6.c(1)(b)10 of VA Handbook 6500, which states that "OI&T is responsible for granting file access. The supervisor and/or application coordinator will determine the needs of each user and the appropriate degree of access authority to be assigned." According to (b) (7)(C), this paragraph meant that (b) (7)(C), as the (b) (7)(C) had the authority to grant whatever access was necessary for these employees to do their jobs.

(b) (7)(C) also said that the limitations of the software meant that the VHA employees needed an elevated level of access to perform their duties. He explained that SQL is "is not always the best in allowing delineation or granularization of duties or permissions to allow [a user] to do certain functions," and that if a user needed to run reports using the entire database, he or she would need access to the entire database, which would require the user to either be a SQL administrator, meaning that they have administrative rights to the entire database, or be an administrator for the server itself. (b) (7)(C) said that "in a perfect world, where you have granularization down to the bit level," it would not be necessary for the VHA employees to have that type of access in order to build reports. However, that kind of functionality was not built into the operating system and version of SQL they were using at that time (2008-2009). For this reason, the VHA employees required elevated privileges in the DW system in order to build data and run reports.

(b) (7)(C) said that contractors working under the direction of OI&T were considered OI&T staff for the purposes of VA Handbook 6500. He said that it is "typical" for contractors to have programmer or administrative accounts on VA systems and he did not see any problems with contractors having such access to the data warehouse system.

(b) (7)(C) also said that he saw no significant risk in allowing contractors and VHA employees to have elevated access to the data warehouse system. He explained that VHA employees and contractors go through a background investigation at the appropriate level for the data they are working with – in most cases, a regular background investigation for access to information of moderate to high sensitivity – and that VA employees and contractors must adhere to the VA National Rules of Behavior, which require that they use their access only for authorized and official duties and access only that data which is needed to fulfill their duties.

(b) (7)(C) said that (b) (7)(C) consulted with her before giving VHA employees elevated access to the data warehouse system and that she concurred with (b) (7)(C) decision to give these employees elevated access. (b) (7)(C) said that she told (b) (7)(C) that, as far as she knew, there was no prohibition against giving elevated privileges to someone outside OI&T, although such access was not routine.

(b) (7)(C) told us that non-OI&T employees were allowed to have elevated access to VA information systems if they needed such access to do their jobs. However, such access had to be justified, and the CIO and ISO had to agree that the access was required. (b) (7)(C) also said contractor employees working under a contract with OI&T were considered OI&T employees for the purposes of system access.

(b) (7)(C) also told us that she did not believe that VA Handbook 6500, paragraph 6c(2)(b)1.h. prohibited anyone who is not an OI&T employee from having elevated privileges. She said that four or five years ago, the VA Central Office directed an overall review of system accesses and that, following this review, OI&T did not require elevated privileges be removed from anyone who was not an OI&T employee. Rather, they required supervisory, ISO, and CIO approval for non-OI&T personnel to continue to hold elevated access. For example, some clinical informatics staff was allowed to keep elevated access because they needed such access to do their work.

(b) (7)(C) also cited the OI&T Operations Administrative Rights Management Handbook, which requires restricting administrative or other high-level access whenever there is no "authorized business need for possessing these rights." The Handbook also states that it is "not the intent [of this policy] to disrupt any business activity; rather for OI&T to ensure that only role-based access is granted based on least privilege principles, enabling all authorized users to have the appropriate access to perform their duties but no more."

When asked whether non-OI&T employees having elevated access to the data warehouse system posed any security risk, (b) (7)(C) said that a major risk for operational (hospital) systems is that, if the system is brought down, people cannot do their jobs and patients cannot be treated. However, she said that this was not a risk for the data warehouse system, which takes information from the operational (hospital) systems and puts it in a data "warehouse" so that users could run reports. (b) (7)(C) (b) (7) said that the real risk in this case was the release of sensitive patient information, which is essentially the same risk as a medical center employee having access to patient records on their computers. She said, however, that the VHA and contractor employees received background checks and completed the required security training to minimize this risk. Also, in accordance with VHA Handbook 1600, each contractor had to sign a "business associate security agreement" governing contractor use, disclosure, and protection of protected health information (PHI).

(b) (7)(C) told us that when the VHA employees were granted elevated access to the data warehouse system, written justification was not required. However, she said that (b) (7)(C) recently initiated a new standard operating procedure requiring written justification and approval by the program manager or supervisor, the Network ISO, and the Network CIO before granting elevated access to VISN 5 information systems. This approval must be renewed annually.

Alleged Prohibited Personnel Practices

We investigated an allegation that (b) (7)(C) violated Merit System principles and gave preferential treatment to a candidate for employment by selecting a favored candidate for a (b) (7)(C) position over a more qualified candidate. (b) (7)(C) denied that she was involved in the selection process for the (b) (7)(C) (b) (7)(C), which was a VHA position. (b) (7)(C) works within OI&T.

We found that (b) (7)(C) was not the decision-maker for this hiring action. Records provided by the VISN 5 Human Resources Office (HRO) reflect that (b) (7)(C) (b) (7), and not (b) (7)(C), was the selecting official for the (b) (7)(C) (b) (7)(C), (b) (7)(C), who no longer works for the VA, selected the incumbent from a certificate of three eligible candidates provided by the HRO.

Conclusion

We found that (b) (7)(C) did not give preferential treatment to a Hitachi employee by allowing him to Telework after she denied Telework privileges to another contractor employee. Rather, we found (b) (7)(C) and (b) (7)(C) turned down the other contractor employee's Telework request because they wanted all the DW team members to work on site when the project was in its early stages. (b) (7)(C) later allowed the Hitachi employee to Telework because the project was at a more mature stage, making Telework more feasible. At about the same time, (b) (7)(C) allowed the employee of another contracting company to Telework. In both cases, the contracting officer executed a contract modification to allow the contractor employees to Telework.

We found that that (b) (7)(C) did not give preferential treatment to contractor Hitachi Consulting by allowing the company to assign an unqualified employee to the VISN 5 DW project. (b) (7)(C) was not the sole decision maker in this case. Rather, she served on a panel of DW team members who interviewed the Hitachi employee and found that he was qualified for the SSRS task. The panel also declined to accept other Hitachi candidates who lacked the required skills.

We found that (b) (7)(C) did not misuse Government resources by giving a Key Logic employee on-the-job training in commercial software packages (SQL Server Reporting Services (SSRS), SharePoint, and PerformancePoint). Witnesses told us that they never observed the Key Logic employee, who was proficient in these software packages; receive on-the-job training while assigned to the DW project.

We found that (b) (7)(C) did not misuse Government resources by sending the Key Logic employee to VA-sponsored IT training. We found that (b) (7)(C) sent the Key Logic employee to TFS training and proposed paying one half the employee's travel costs because this training was for the benefit of the Government. The contracting officer executed a contract modification authorizing this expense.

We found (b) (7)(C) did not violate contracting/procurement regulations by allowing contractor employees to perform work outside their task orders. When the issue was brought to (b) (7)(C) attention, she sought advice from the contracting officer, who told (b) (7)(C) that this practice was permissible and executed contract modifications to allow contractor employees to perform work on a range of tasks within the data warehouse project.

We found that (b) (7)(C) did not violate VA information security policy by granting non-OI&T (VHA and contractor) employees elevated access to the data warehouse system. (b) (7)(C) believed that VHA Handbook 6500, paragraph 6c(2)(b)1,h, bars non-OI&T employees from having elevated (programmer and/or system administrator) access to VA information systems. However, other VA policies indicate that (b) (7)(C) had the authority to grant elevated access to non-OI&T employees if the employees needed such access in order to perform their duties. In particular, the OI&T Operations Administrative Rights Management Handbook requires restricting administrative or other high-level access "only when there is no authorized business need for possessing these rights." The Handbook further states that OI&T is to grant access "based on least privilege principles, enabling all authorized users to have the appropriate access to perform their duties but no more."

We found that (b) (7)(C) did not engage in a prohibited personnel practice, as she was not the decision-maker for the hiring action. Records provided by the VISN 5 Human Resources Office (HRO) reflect that (b) (7)(C), and not (b) (7)(C), was the selecting official for the (b) (7)(C) position.

We did not substantiate the allegations against (b) (7)(C). Therefore, we are closing this investigation without issuing a formal report or memorandum.

Prepared by (b) (7)(C) 1/30/13
Date

Approved by (b) (7)(C) 1/30/13
Date