

Appendix B—Organizational Conflict of Interest Avoidance Plan [L.22(3)]

B.1 Introduction

The CSC Team will implement an aggressive Data Handling Program that addresses two tightly coupled components: (1) preventing misuse of sensitive data by SP employees, and (2) preventing unauthorized access to sensitive data by NASA managers, NASA employees, or the General Public. This COI Avoidance Plan addresses the first issue. We elaborate on the second component in our Data Handling Plan in Appendix C of this Contract Volume.

CSC's execution of NSSC Service Provider functions and responsibilities could create the appearance of an Organizational Conflict of Interest (OCI), as defined in FAR Part 9.5. The purpose of this document is to institutionalize an Organizational Conflict of Interest Avoidance Plan that will ensure that the CSC NSSC Team avoids both actual and perceived Organizational Conflicts of Interest. CSC's OCI Avoidance strategy is to raise the awareness of OCI for all CSC Team employees and NSSC management through education programs, to install processes and procedures that discourage or prohibit actual OCI events, and to record, document and flag for review any transactions that could be viewed as questionable by external auditors. CSC's believes that OCI can be avoided if:

- a. CSC Team employees are trained in identifying potential OCI circumstances
- b. NASA Managers are also trained in identifying potential OCI circumstances
- c. CSC Team documents processes that are of highest OCI risk potential
- d. CSC Team develops processes to isolate and track transactions with high OCI potential
- e. NASA, CSC and all Team Members conduct internal audits and reviews to monitor compliance

We have identified the following potential areas that may create the appearance of an OCI:

1. Access to "Confidential Information" (RFP Clause G8)
2. Handling of third party data that the Government has agreed to handle under protective arrangements (RFP Clause H.6)
3. Handling of third party data with limited or restricted rights (RFP Clause H.6)
4. Handling of data that the Government intends to control (RFP Clause H.6)
5. Handling of data that falls into protected categories (technical data, privacy act data, computer software, generated test data, administrative, management information or financial data, including cost or pricing data) (RFP Clause H.6)
6. Review and Payment of Contractor Invoices, including those of CSC and its teammates. (PWS Section 3.1.1.1)
7. Review and Payment of Grants (PWS Section 3.1.1.2)
8. Human Resources privacy data review and release (PWS Section 3.2)
9. Procurement data (competition sensitive) (PWS 3.3)

10. Training Purchases (CSC Team training for NASA) (PWS 3.2.2)
11. Payroll time and attendance processing (PWS 3.1.3), travel services (PWS 3.1.5), administration of drug testing (PWS 3.2.1), benefits processing (PWS 3.2.3) for NASA employees who may be friends or relatives of NSSC Team employees
12. Review and reconciliation of Reporting NASA Contractor-held Property (PWS 3.1.4) for contracts held by any NSSC team member.

B.2 Background

The intent of the NASA Shared Services Center (NSSC) Service Provider contract is to provide transactional and customer support services to NASA stakeholders for major administrative functions, including financial management, human resources and procurement. The Service Provider is the primary operational services contractor at the newly established NSSC, which is organizationally a separate NASA Center.

The Scope of the NSSC SP contract requires access to streams of incoming data that are of varying levels of sensitivity, including privacy data, fiduciary data, contractor proprietary data and other sensitive data, including ITAR data. In addition, daily functional activities require continuing access to NASA data warehouses, both centrally located and virtual. The NSSC SP services are all support activities that are appropriate for delegation to and execution by a contractor. Civil Service employees will continue to execute those functions that are “inherently Governmental,” such as voucher certification and payments and invoice certification. However, in the course of day-to-day business, NSSC SP employees will be required to review, analyze and process documents (or their electronic equivalents) that require special procedural considerations to avoid the appearance of any conflict of interest. Essentially all functions assigned to the SP will involve access to, processing of, or release of sensitive but unclassified data in all categories.

B.3 CSC Corporate Philosophy

CSC has long had as one of its foremost Management Principles the commitment that “We will conduct our business strictly in accordance with all laws and regulations of the country in which we are doing business.” Implicit in that principle is that we require our employees and our subcontractors and teammates to conform to all laws, regulations, and procedures under which our clients operate as a condition of their employment. Specifically, we require all of our employees to sign a “Covenant Against Disclosure” as a condition of their employment, and we require subcontractors to demonstrate a similar process. The appropriate paragraph relating to this topic reads as follows:

Covenant Against Disclosure: In addition to all obligations with respect to observance of U.S. Government security regulations, I understand that it may be desirable and necessary for CSC or any of its suppliers, licensors, or customers, to disclose to me information related to the technology know-how, products, and business data of CSC or its suppliers, licensors or customers, and I therefore agree as follows:

“I agree to accept and retain such data or information in confidence and agree, at all times during and after the termination of my employment, not to disclose or reveal such data or information, nor to use, copyright, or patent such data or information, without the prior written consent of the president of the division or

business unit of CSC or his designee. I also agree to keep the contractual relationships of CSC with its suppliers, licensors, licensees, customers, contractors and subcontractors confidential, including the names, addresses, or special requirements of CSC's customers".

This basic principle is also documented in CSC's published handbook policies, which state "it is the policy of Computer Sciences Corporation Federal Sector to safeguard from disclosure... the proprietary data of our customers, subcontractors, and other companies..."

Our Chief Operating Officer recently reiterated our corporate commitment to protecting client data in a letter to all CSC employees, presented in Exhibit B-1.

In addition to ensuring that our employees do not engage in any malfeasance or conflicts of interest, we also work with each client to ensure that we avoid situations that might generate the appearance of any malfeasance or conflict of interest. In particular, in the Federal Government contracting arena, we are very careful to ensure that our support employees do not deliver "personal services." We train them and their managers in appropriate ways to segregate themselves from direct supervision from our Civil Service clients and technical monitors. We also educate both employees (and sometimes our clients) on the definition of "inherently governmental" roles and functions to help both of them avoid inadvertent assignment of inappropriate task assignments.

Finally, CSC has a published Organization Conflict of Interest policy to ensure that all applicants for employment are screened to avoid any actual or potential OCI. That policy will play a prominent role in the NSSC SP contract, for which we plan to hire NASA Civil Servants who have been displaced as a result of the implementation of the NSSC. In accordance with our policy, we will require NASA to provide a formal post-employment clearance for each senior NASA Civil Servant that they identify to us as "displaced," before we can extend an offer of employment.

Each of our teammates and subcontractors has similar provisions and has agreed to abide by the provisions of this OCI Avoidance Plan. All of the above policies are available for your review upon request.

B.4 Specific Situations at NSSC

- a. Review of Contractor Invoices (other than CSC or CSC team members):** In support of the Accounts Payable functions, the CSC SP Team will be required to review invoices submitted to the NSSC for payment from all NASA contractors. Those vouchers may contain proprietary financial data belonging to potential competitors of CSC or its teammates. The invoices may also contain information about specific contracts that CSC or its team mates may want to bid on in the future.

Protecting Our Future – CSC Launches Information Security Awareness Program

CSC must protect the substantial amount of sensitive and official internal and client information for which we are responsible worldwide. Ensuring the security of this information from unauthorized access is an ethical obligation and a legal requirement, as is ensuring the integrity and availability of our information resources and services.

Failure to adequately protect our information from unauthorized access, modification, disclosure and/or destruction introduces significant risk, as well as the prospect of loss of customer and shareholder confidence, competitive advantage and jobs. Therefore, it is imperative for all of us, as CSC employees, to understand the requirements, responsibilities and our own role in helping to protect our future by securing the company's information infrastructure and assets.

While information technology and its benefits have enabled us to process information in ways never before envisioned, this technology also can leave CSC vulnerable to potential harm such as sabotage, fraud, theft, vandalism, information capture and misuse. In order to effectively manage and avoid any such harm in the future, CSC has developed a Global Security Awareness Program, to highlight our existing security policies and provide practical guidelines and advice on how all employees must do their part to safeguard our information assets.

As part of this initiative, all employees are required to practice the skills and principles established by the program as we go about our daily activities. In addition, new employees will undergo an initial security orientation or awareness training within the first two months of employment, and annually thereafter, along with all current CSC employees.

Over the coming months, all CSC employees will receive communications on various aspects of this program. A CSC Portal page currently is under development to improve the ease of access to relevant security information across CSC globally.

As we move forward with this vital program, it is my expectation that information security will be recognized as one dimension of everyone's job, and not simply something that is the responsibility of security personnel or experts performing security work. Our future success depends on our ability to meet our legal and ethical obligations to our customers, our shareholders, and our employees.

Over the coming weeks, you will hear more about this important program. I encourage you to report anything that you identify as potential security weaknesses, and to submit any comments or suggestions you have regarding the continuous improvement of our information security policies or practices to the CSC Information Security Officer by sending an email to ciso@csc.com.

Michael W. Laphen
President and Chief Operating Officer

*Exhibit B-1. CSC's Information Security Awareness Program
Safeguarding the proprietary data of our customers is a CSC corporate commitment.*

Proposed Solution Relative to Potential OCI and Protection of proprietary

Information: CSC will require every CSC Team employee who is assigned to the FM or Procurement processing functions Invoice Review Team to participate in a special awareness training shortly after award of the contract that addresses Conflict of Interest Avoidance and to sign an additional Conflict of Interest Avoidance Agreement that reads as follows:

“I further understand that in the performance of my official duties, I will be reviewing data that is fiduciary, proprietary, private and/or sensitive, from other contractors and vendors doing business with NASA. I agree that at all times during and after the termination of my employment with the respective CSC Team member, to utilize those data only for the purposes intended in the execution of my official duties, and I agree not to disclose or reveal such data or information unless specifically directed in writing by the NASA Contracting Officer or an equivalent NASA official.”

This training will be refreshed on an annual basis, and the certification and training materials will be provided to any new hires after the inception of the contract.

- b. Review CSC Team Partner Vouchers:** In support of the FM processing functions, the CSC Team will review contractor invoices that originated with CSC or their team mates or one of their subcontractors. Though we would not be certifying these invoices for payment based on the proposed solution, the appearance of an OCI could nevertheless be created.

Proposed Solution: CSC and NASA will take procedural steps to avoid creating any perception of an opportunity for Conflict of Interest in processing invoices from CSC or its team mates by executing the following actions:

- a. The CSC Team will ensure that its processes include a clear demarcation for “inherently governmental” actions.
- b. The CSC Team will maintain a written log of all invoices that originate with CSC or its Teammates or subcontractors, and will make the log available for review and audit upon request.
- c. CSC Team internal auditors will audit the logs and transactions randomly to ensure compliance. Government auditors are encouraged to also perform periodic compliance reviews.
- c. Review and use of Personal and Competition Sensitive Data:** Performance of the NSSC HR functions will require that CSC or its teammates access and utilize personal data from HR data warehouses to respond to employee requests for information. Performance of the NSSC Procurement functions will require that CSC or its teammates access and utilize competition sensitive data from financial and procurement warehouses to process transactions and respond to authorized requests for information.

Proposed Solution Relative to Potential Misuse of Competition Sensitive and

Privacy Data: CSC will require every NSSC Team employee who requires access to NASA HR Private data or NSSC Competition Sensitive data to participate in annual awareness training that addresses Conflict of Interest Avoidance and to sign an additional Conflict of Interest Avoidance Agreement that reads as follows:

“I further understand that in the performance of my official duties, I will be reviewing data that is fiduciary, proprietary, private and/or sensitive, from other contractors and vendors doing business with NASA. I agree that at all times during and after the termination of my employment with the respective CSC Team member, to utilize those data only for the purposes intended in the execution of my official duties, and I agree not to disclose or reveal such data or information unless specifically directed in writing by the NASA Contracting Officer or an equivalent NASA official.”

B.5 Applicability of Plan

This plan is applicable to CSC and all of its teammates and subcontractors who may work on the NSSC SP contract.

B.6 Addendums

Addendum No. 1 (February 3, 2009)

CSC believes that the current Organizational Conflict of Interest (OCI) plan is a sound plan; however with the NASA Agency Consolidated End-User Services (ACES) and other similar I3P requests for proposal to be issued in the near future, CSC is providing proactive precautionary measures to avoid any potential, apparent or actual OCI. The services associated with the Tier 1 Helpdesk have been determined to fall within the scope of the Performance Work Statement (PWS) at the NSSC. Planning and supporting the Tier 1 Helpdesk may be perceived as an unfair competitive advantage and because performance of the NSSC PWS requirements may require that CSC or its team subcontractors access and utilize data from financial and/or procurement data warehouses that may be sensitive data, CSC is executing the following actions.

Proposed solution relative to potential access to competition sensitive and privacy data:

During February and March 2009, CSC will require every NSSC Team employee in all service areas to participate in an OCI refresher course. The OCI refresher course will reinforce that CSC and team subcontractor employees may not disclose sensitive information obtained during their employment at the NSSC. All employees will be required to review and sign a revised Non-Disclosure Agreement which will be archived for audit purposes.

CSC will determine which team subcontractors will be involved with any I3P acquisitions and their potential teaming situations. When this information is received, a review will be conducted to determine if additional OCI risk mitigations need to be added to our OCI plan.

Additionally, when the PWS for the Tier 1 Helpdesk is provided to CSC and the RFPs for the ACES or any I3P are formally released to the public, CSC will review those

requirements to determine the need for additional OCI risk mitigation, and incorporate them in the current OCI plan as required.

Addendum No. 2 (May 20, 2009)

CSC implemented the OCI Refresher training course on April 15, 2009 to all CSC and team Subcontractor employees including the resigning of an updated Covenant Against Disclosure form. This is a mandatory employee participation requiring 100% completion that was completed on May 20, 2009. Since February 2006 the NSSC/CSC has conducted eight (8) Personal Awareness training sessions for all NSSC employees that included Organizational Conflict of Interest, Handling of Data and Personal Services awareness

All of the team subcontractor subcontracts contain Section H.14(a) which states

“H.14 STANDARD OF CONDUCT AND RESTRICTIONS

The Seller shall adhere to the same professional and ethical standards of conduct required of Government/Buyer’s personnel. The Seller shall not:

- a) Discuss with unauthorized persons any information obtained in the performance of work under this contract .”

This is not new subcontract language but just a reminder of what the subcontracts contain.

Lockheed Martin worked jointly with CSC on an effort to update their OCI Plan with strict adherence to the new requirements at the NSSC. The updated plan was discussed and provided to all the LM employees at the NSSC.

On February 5, 2009 the CSC Acting Vice President of the North American Sector, Civil Division, Science and Engineering Services issued an e-mail firewalling the lead team supporting the I3P RFP from any contact with CSC and the team subcontractors at the NSSC. Since that time, all of the CSC employees who have any potential dealings with the I3P RFP’s have been firewalled from the CSC and team subcontractor employees at the NSSC. Additionally, on March 12, 2009 CSC notified and requested that all the team subcontractors follow the firewall approach with their companies and their employees at the NSSC as well.

Effective May 6, 2009, the President of North American Public Sector, Civil and Health Services Group has provided full authority to the NSSC CSC Program Manager to approve and submit the CO# 28 proposal for the Tier 0/1 Enterprise Service Desk and Enterprise Service Ordering System locally at the NSSC organization. This guarantees that the proposal’s integrity will remain locked at the NSSC.

CSC is currently in the process of implementing a new exiting process for employees who have terminated their employment at the NSSC which includes the signing of an

acknowledgement form that reiterates the meaning of their signature on the Covenant Against Disclosure.