City of New York

OFFICE OF THE COMPTROLLER

Scott M. Stringer
COMPTROLLER

AUDITS AND SPECIAL REPORTS

IT AUDIT

Marjorie Landa

Deputy Comptroller for Audit

Audit Report on the Development and Implementation of the Senior Tracking, Analysis and Reporting System Administered by the Department for the Aging

SI15-121A

June 23, 2016

http://comptroller.nyc.gov

THE CITY OF NEW YORK
OFFICE OF THE COMPTROLLER
1 CENTRE STREET
NEW YORK, NY 10007

SCOTT M. STRINGER
COMPTROLLER

June 23, 2016

To the Residents of the City of New York:

My office has audited the New York City Department for the Aging's (DFTA) Senior Tracking, Analysis and Reporting System (STARS) to determine whether the application meets the overall goals as stated in the system specifications, has adequate functions to ensure the information process is reliable, and is secure from unauthorized access. We perform audits of New York City agencies such as DFTA as a means of ensuring that City agency information systems and resources are cost effective, efficient, secure, and operate in the best interest of the public.

The audit determined that the overall goals of STARS as stated in the system specifications have generally been met. STARS provides a centralized system to share client information between DFTA and its contracted service providers. However, our audit found that during the system development stage, DFTA did not fully comply with the rules of the New York City Procurement Policy Board (PPB Rules) and with the Department of Information Technology and Telecommunications' (DoITT) policies. We also found some security control weaknesses. Specifically, STARS users were not required to periodically change their passwords, multiple users shared one account, and inactive employees' accounts were not disabled immediately. Further, we found system deficiencies that could affect the security and accuracy of client data, including unexpected user log outs, the ability to enter future dates for past events, and the existence of duplicate client records.

The audit makes 17 recommendations that, if implemented, should mitigate the stated system security weaknesses and enhance access controls. These recommendations included that that DFTA correct the security controls weakness, such as password controls and account sharing. The audit further recommends that DFTA remediate the system deficiencies, such as unexpected log outs and duplicate client records.

The results of the audit have been discussed with DFTA officials, and their comments have been considered in preparing this report. Their complete written response is attached to this report.

If you have any questions concerning this report, please e-mail my Audit Bureau at audit@comptroller.nyc.gov.

Sincerely,

Scott M. Stringer

TABLE OF CONTENTS

THE CITY OF NEW YORK
OFFICE OF THE COMPTROLLER
AUDITS AND SPECIAL REPORTS
IT AUDIT

Audit Report on the Development and Implementation of the Senior Tracking, Analysis and Reporting System Administered by the Department for the Aging

SI15-121A

EXECUTIVE SUMMARY

We audited the New York City (the City) Department for the Aging's (DFTA) Senior Tracking, Analysis and Reporting System (STARS) to determine whether the application meets the overall goals as stated in the system specifications, has adequate functions to ensure the information process is reliable, and is secure from unauthorized access.

DFTA is charged with promoting the independence, health and well-being of senior New Yorkers through advocacy, education, and the coordination and delivery of services. DFTA receives federal, state and city funds for these purposes. These funds are distributed by DFTA through contracts with over 500 direct service providers. DFTA services include hot meals and activities at Senior Centers, home-delivered meals, case management, home care, transportation, and legal assistance.

In July 2012, DFTA contracted with PeerPlace Networks LLC (PeerPlace) to customize their data management software into a single product called STARS to replace two computer systems. STARS is an internet-based system developed to manage and track client services. It contains one master client database that serves as the central repository of information for all connected service providers. STARS also contains modules tailored for specific services, such as preparing client route information for home delivery meals and tracking attendance at Senior Centers. Authorized users can create client profiles, update client data, send referrals to other programs, and run reports based on their privilege level. STARS was implemented in April 2013 at Senior Centers, and expanded to other service providers soon after.

Audit Findings and Conclusions

Our audit found that the overall goals of STARS as stated in the system specifications have generally been met. STARS provides a centralized system to share client information between DFTA and its contracted service providers. However, we found that during the system

development stage, DFTA did not comply with the rules of the New York City Procurement Policy Board (the PPB Rules) in connection with changes that were made to the contract deliverables. In addition, we found that DFTA failed in its implementation of STARS to comply with the Security Accreditation Process, a citywide Department of Information Technology and Telecommunications (DoITT) policy. We also found security control weaknesses in STARS, including that users are not required to periodically change their passwords, multiple users shared one account, and inactive employees' accounts were not disabled immediately. Further, we found system deficiencies that could affect the security and accuracy of client data, including unexpected user log outs, the ability to enter future dates for past events, and duplicate client records.

Audit Recommendations

To address these issues, we made 17 recommendations including that DFTA should:

- Ensure any future contract changes are made in full compliance with the PPB rules.
- Ensure that STARS complies with DoITT's Citywide Security Policies and Standards.
- Require STARS users to comply with DoITT's Password policy.
- Ensure all terminated or inactive employee accounts are immediately deactivated from STARS.
- Review all accounts and ensure that STARS users are granted only the minimum level of privileges necessary for them to perform their job functions.
- Restrict STARS administrators' access to their assigned jurisdiction only.
- Work with PeerPlace to identify and resolve the condition that's causing unexpected user logouts.
- Work with PeerPlace to implement an event modification feature in the software, and create a policy and procedure for deleting/correcting erroneous event entries.
- Work with PeerPlace to ensure that all date fields are validated prior to accepting data entry.

Agency Response

In its response, DFTA generally agreed with the audit's findings and the recommendations. The agency stated, "DFTA will be following up on these recommendations as it continues its ongoing work to further enhance and improve STARS functionality."

AUDIT REPORT

Background

DFTA is charged with promoting the independence, health and well-being of senior New Yorkers through advocacy, education, and the coordination and delivery of services. DFTA receives federal, state and city funds for these purposes. These funds are distributed by DFTA through contracts with over 500 direct service providers that help New York City seniors maintain or enhance their quality of life. DFTA services include hot meals and activities at Senior Centers, home-delivered meals, case management, home care, transportation, and legal assistance.

To track, manage, and report the provision of client services, until April 2013 DFTA used two different computer systems, Provider Data System (PDS) and Senior Participant Profile (SPP). However, these systems did not interface with one another to exchange client information. As a result, service providers did not have uniform client information. In July 2012, DFTA contracted with PeerPlace, a software developer, to customize their data management software into a single product called STARS to replace PDS and SPP.

STARS is an internet-based system developed to manage and track client services. It taps one master client database that serves as the central repository of information for all connected service providers. STARS also contains modules tailored for specific services, such as preparing client route information for home delivery meals and tracking attendance at Senior Centers. Authorized users can create client profiles, update client data, send referrals to other programs, and run reports based on their privilege level.

STARS was implemented in April 2013 at Senior Centers, and expanded to other service providers soon after. The initial STARS contract covered the period from July 2012 to June 2014 and cost approximately $2.3 million. The contract provided for the system's development, implementation, and maintenance. It also provided 2,150 licenses available to DFTA and its service providers. In July 2014, the contract was renewed for approximately $2.66 million for five years. The renewal contract covers the period from July 2014 through June 2019, and includes the software's usage, technical support services, and future enhancements. PeerPlace administers STARS based on DFTA's specifications. DFTA is responsible for communicating policies, protocols, and standards for STARS use. This includes DFTA's policies and procedures as well as the city-wide policies established by DoITT.

As the City agency charged with overseeing information technology (IT) and telecommunications for more than 120 City agencies, boards, and offices, DoITT provides assistance to help deliver efficient, effective and secure IT services, infrastructure, and telecommunications. Among other things, DoITT provides security expertise and services to protect City data and IT assets through management of security infrastructure, policies, and standards. DoITT also provides leadership for the accreditation of new systems and applications commissioned for use at various City agencies. Towards that end, the agency provides guidance for re-accreditation, as well as a mechanism for agencies to request exceptions to policy. All City agencies and employees, as well as all contractors and vendors doing business with the City, are required to follow these policies and standards.

Objectives

The objectives of this audit were to determine whether STARS:

1. Met its overall goals as stated in the system specifications;
2. Has adequate functions to ensure the information process was reliable;
3. Is secure from unauthorized access.

Scope and Methodology Statement

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, and appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on the audit objectives. This audit was conducted in accordance with the audit responsibilities of the City Comptroller as set forth in Chapter 5, §93, of the New York City Charter.

The scope of this audit was from the implementation of the system in April 2013 to February 2016. We conducted fieldwork from October 2015 to February 2016. Please refer to the Detailed Scope and Methodology at the end of this report for the specific procedures and tests that were conducted.

Discussion of Audit Results

The matters covered in this report were discussed with DFTA officials during and at the conclusion of this audit. A preliminary draft report was sent to DFTA and discussed at an exit conference held on May 31, 2016. On June 2, we submitted a draft report to DFTA with a request for comments. We received a written response from DFTA on June 16, 2016. In their response, DFTA officials generally agreed with the audit's findings and recommendations. The agency stated, "DFTA will be following up on these recommendations as it continues its ongoing work to further enhance and improve STARS functionality."

The full text of the DFTA response is included as an addendum to this report.

FINDINGS AND RECOMMENDATIONS

STARS is currently operational and generally meets its overall system specification goals. It provides a centralized system to share client information between DFTA and its contracted service providers. However, we found that during the system development stage, DFTA did not comply with the PPB Rules regarding changes that were made to the contract deliverables. Additionally, in implementing STARS, DFTA failed to comply with the Security Accreditation Process, a Citywide DoITT policy. We also found security control weaknesses in STARS, including that STARS users are not required to change their passwords periodically, multiple users shared one account, and general users were granted administrator privileges. These weaknesses increase the risk of unauthorized access to client information, including personally identifiable information (PII). Further, we found system deficiencies that could affect the security and the accuracy of client data, including unexpected user log outs, the ability to enter future dates for past events, and duplicate client records.

Non-Compliance with PPB Rules

We reviewed the STARS system specifications and found that while DFTA approved changes to the contract deliverables, it failed to follow the PPB Rules and memorialize these changes in writing through the City's change order process. The PPB Rules were established to ensure fairness, safeguard the integrity of the procurement process and protect against corruption, fraud, waste, and abuse in the City's procurement of goods and services. To this end, among other things, the PPB Rules impose contract management practices on City agencies that are designed to help ensure that vendors are paid only for work they actually perform and that they perform all the work they are paid for.

We found that DFTA eliminated three components of the original STARS development contract without completing the City's formal change order process: the Home Sharing Program; the Grant Funded Program; and the Home Energy Assistance Program/Weatherization Referral and Assistance Program (HEAP/WRAP). These omitted contract requirements had been budgeted at a cost of $36,050, which was paid to the vendor, notwithstanding the vendor's decreased responsibilities. According to DFTA officials, rather than decrease the funds due to the vendor, the agency reallocated the money to additional STARS enhancements.

Section 4-02(a)(1) of the PPB Rules that govern changes to contract deliverables mandates that "[a]ll changes to existing contracts shall be approved by the ACCO [Agency Chief Contracting Officer] and shall be reflected in a change order, which, once authorized, shall become a part of the original contract." Following the exit conference, DFTA provided documentation that showed additional hours were allocated to other enhancements. However, we cannot determine whether these hours were from the discontinued programs, since these changes were not reflected in the contract. Non-compliance with PPB Rules may place DFTA at risk of mismanaging public funds and deliverables associated with the STARS contract.

Recommendation

1. DFTA should ensure any future contract changes are made in full compliance with the PPB rules.

> ***DFTA Response:*** DFTA generally agreed and stated, "DFTA recognizes that contract changes need to be formally memorialized through the City's change order process. The Department will be mindful of doing so in the future."

Non-Compliance with DoITT's Security Accreditation Process

We found that in its implementation of STARS, DFTA failed to comply with DoITT's Security Accreditation Process, a Citywide review and evaluation process implemented by DoITT to ensure that computer systems utilized by City agencies meet certain security standards. As a result of DFTA's failure to submit STARS to DoITT's Security Accreditation Process, STARS is potentially more vulnerable to a security breach that could affect critical DFTA operations, its contract service providers, and the seniors they serve.

DoITT's policy for the Security Accreditation Process requires that,

> [a]ll externally accessible, public facing applications and internally accessible, multi-agency applications developed to support City of New York business must be built in a secure fashion. These applications must successfully complete the Security Accreditation Process to ensure compliance with security policies, standards and best practices. Successful completion is acknowledged by the Citywide Chief Information Security Officer (CISO) and must be achieved prior to launch in production.[1]

We found that DFTA did not submit documentation to DoITT for STARS' security accreditation review. DFTA officials maintained that DoITT's Security Accreditation Process is not applicable to STARS because, among others things, it is a commercial-off-the-shelf application, and therefore was not built from the ground up. They further maintained that DoITT's accreditation process did not apply to STARS because it is accessible only to service providers and not other agencies. Finally, DFTA stated that before awarding the contract, its security team conducted a review, and no security issues were "flagged."

However, based on the criteria established by DoITT, its Security Accreditation Process would apply to STARS. Specifically, DoITT has determined that where a single agency system is hosted in the "cloud," it is subject to the Security Accreditation Process. Since DoITT does not host STARS and because it is accessed through the Internet, it is considered "cloud-based." Further, as a system that is accessible to its users (DFTA and service providers) via the Internet, it is public facing. According to DoITT's Security Accreditation matrix available on its website for City agencies' reference, if an application or system is hosted in the cloud and is public facing (whether single-agency or multi-agency), accreditation for that application or system is required.

In addition to system accreditations, DoITT requires cloud vendors, such as PeerPlace, to complete the Cloud Vendor Survey in order to ensure that *they* comply with Citywide security policies, standards and best practices. Although DoITT provides for an exception to the policy, the final decision on who is subject to that exception rests with the DoITT Commissioner and the Citywide CISO alone. No such exception was requested for PeerPlace or granted by the Citywide CISO.

Finally, notwithstanding DFTA's claim that its security professionals did not identify any security "flags" in STARS, we found access control concerns and system deficiencies that raise concerns

[1] The Security Accreditation Process outlines key steps to be followed and critical tests to be performed during the development of new systems.

about the security of the system as implemented and utilized by DFTA and its contracted service providers, discussed in more detail below. These issues pose potential system vulnerabilities that might have been identified and rectified during the security accreditation process.

Accordingly, under DoITT's policies and procedures, DFTA should have completed the accreditation process to ensure that adequate system controls were in place. Likewise, DFTA should have instructed PeerPlace to complete the Cloud Vendor Survey.

Recommendations

DFTA should:

2. Ensure that STARS complies with DoITT's Citywide Security Policies and Standards.
3. Ensure all future system developments and enhancements are made in accordance with DoITT policies.

DFTA Response 2 & 3: DFTA generally agreed with these recommendations. It stated that "DFTA has contacted DoITT's Citywide Chief Information Security Officer (CCISO), who oversees the Citywide Cybersecurity Program, for guidance. . .DFTA will be scheduling a follow-up meeting with DoITT in a few weeks for further discussion."

Access Control Issues and System Deficiencies

Adequate controls over system access and continual system monitoring reduces a system's vulnerability to security breaches as well as the opportunity for system misuse. However, the audit found access control weaknesses in STARS. These include:

- users were not required to periodically change their passwords;
- multiple users shared one account;
- former employees' accounts were not immediately deactivated;
- some general users had been granted program administrator privileges; and
- program administrators have the ability to assign access outside of their program authority.

DoITT policies prescribe basic access control standards for City agencies and the service providers who develop and maintain systems for those agencies. The access control weaknesses identified in the audit, which are described in more detail below, indicate that DoITT's security policies may not have been communicated by DFTA to Senior Centers and other service providers, who share the same obligation to comply with DoITT requirements as agency personnel.

Absent compliance with DoITT requirements, there is an increased risk that data maintained on the STARS system could be compromised and, as a result, there is an increased risk of fraud. Senior Centers maintain clients' PII such as date of birth, address and health status in STARS. This information is more vulnerable to improper access where, as we found to be the case with STARS, there are inadequate controls over user access.

We also found system deficiencies in STARS that hinder data integrity and that potentially reduce the protection of personal information, including: STARS logging out unexpectedly mid-session;

its generation of inaccurate license and client attendance reports; an inability to delete erroneous event entries; the allowance of invalid date entries; and duplicate client records. Although we found that STARS achieved its overall system specification goals, these deficiencies hinder the operating efficiency of the system. These access control issues and system deficiencies are described in more detail below.

Access Control

No Password Expiration

DFTA officials informed us that STARS, as developed by PeerPlace, does not require users to periodically change their passwords. DFTA's STARS System General Usage and Access Protocols (Access Protocols) require the appointment of an individual at the service provider site to carry out administrative duties including maintaining user access and the integrity of the client data. However, this policy does not require passwords to be periodically changed.

DoITT's Password policy mandates that passwords must be changed every ninety days and must not be reused for four iterations. Adequate password management provides controls over data security to deter the threat of unauthorized exposure to the personal information STARS collects and stores.

DFTA officials were aware of this issue, and requested that PeerPlace incorporate the periodic password change in its May 2016 system enhancement.

Shared User Accounts

We found that DFTA lacks central access control management over its contract service providers that has led to user account inconsistencies. Enhanced management oversight and enforcement by DFTA of STARS policy could reduce the risk of access control vulnerabilities. Among other things, we observed multiple users sharing a single account at 3 of the 14 sampled service providers that we visited. The practice of sharing user accounts increases a risk that changes to client's personal data could be made that could not be traced to a specific user. This is contrary to STARS Access Protocols and DoITT's security policy.

In addition, we found that a program administrator at one service provider authorized several users to have identical passwords, which is also against DoITT's Password Policy. We also found that one service provider allowed multiple user accounts to share the same email address. This practice poses a significant security risk because users can reset passwords through their common email address and thereby gain access to each other's accounts. Sharing the same email account for password reset notification is, in effect, the equivalent of sharing passwords. It is not only contrary to DoITT policy, but to STARS policy as well, which expressly provides that, "[t]o protect the integrity of the data entered into the system, User IDs and passwords are not to be shared. All passwords are to be treated as sensitive and confidential."

Accounts Not Immediately Disabled

We found that DFTA did not ensure all terminated or inactive employees were deactivated from STARS immediately and thereby the risk of improper disclosure of personal information is increased. Specifically, we found four terminated employees' access that had not been disabled immediately in our visits to a sample of contract service providers, which creates serious security concerns. Since STARS is web-based, it can be accessed from any location with an Internet connection. The failure to disable the access of former employees increases the possibility of unauthorized access to client personal information and unauthorized dissemination.

DFTA assigns administrator privileges to at least one individual at each provider location to oversee user accounts and manage STARS. These program administrators are responsible for activating employee accounts, and for immediately deactivating user access upon employment termination. STARS Access Protocols mandate that “access to STARS is immediately removed for all persons who are no longer employed by or under contract with the program.”

User Access and Administrator Privileges Insufficiently Restricted

STARS Access Protocols grant program administrators the ability to assign and remove user access roles within their program. However, during our field observation, we found three instances where general users were granted administrator privileges. Allowing general users to have administrator privileges enables them to modify the access rights of others, which includes adding and deleting users, assigning privileges, and deleting clients’ case notes. Failing to properly limit this access increases the risk of data security breaches.

In addition, we found that all program administrators have the ability to assign users to programs outside of their authority, which potentially grants unnecessary access to client information. Without proper access management and controls, the client information would be at risk of unauthorized disclosure.

Recommendations

DFTA should:

4. Require STARS users to comply with DoITT’s Password policy.

DFTA Response: DFTA agreed with this recommendation. “PeerPlace will implement an automatic 90-day password expiration where the same password cannot be reused for four or more iterations.”

5. Enforce Access Protocols regarding users sharing accounts, and periodically perform assessments to ensure users comply with appropriate access controls.

DFTA Response: DFTA agreed with this recommendation. ”Commencing prior to this audit, DFTA has been working on a STARS Program Administrators Guide. This Guide will reiterate DFTA’s STARS’ Usage Policy and strict prohibition on sharing user names and passwords. DFTA will post this Guide directly on STARS for user access. DFTA will also be including the STARS usage policy in program standards as part of the assessment.”

6. Notify all service providers of the Access Protocols, and instruct the providers to (1) discontinue the practice of setting user accounts with the same password immediately, and to (2) discontinue the practice of allowing multiple users to share the same email address immediately.

DFTA Response: DFTA agreed with this recommendation. “This recommendation will be incorporated into DFTA’s STARS Usage Policy. Instructions to providers will be drafted and released immediately. DFTA is currently working on implementing this recommendation."

7. Ensure all terminated or inactive employee accounts are immediately deactivated from STARS.

DFTA Response: DFTA agreed with this recommendation. "DFTA will reiterate to providers the security risks that are posed when former employees are not immediately inactivated form STARS."

8. Review all accounts and ensure that STARS users are granted only the minimum level of privileges necessary for them to perform their job functions.

DFTA Response: DFTA agreed with this recommendation. "DFTA will incorporate this recommendation into the DFTA STARS Usage Policy. Instructions to providers will be drafted and released immediately."

9. Restrict STARS administrators' access to their assigned jurisdiction only.

DFTA Response: DFTA agreed with this recommendation. "Prior to this audit, DFTA recognized that this restriction is needed. DFTA has been working with the software vendor on this restriction."

System Deficiencies

STARS Unexpectedly Logs Out Users in Mid-Session

We found that STARS unexpectedly logged out users while in mid-session and generated an incorrect message concerning the log-out condition. This problem was repeatedly reported among the STARS users we interviewed and was similarly reported on a User Satisfaction Survey that we distributed to all current users. Users complained that this problem resulted in redundancy of work effort and loss of time. This issue is of particular concern when program users are actively interviewing clients and recording their responses. STARS was created to increase efficiency when providing services to seniors, however, this issue has hindered the work progress.

Incorrect Reporting May Lead to Misallocation of Resources

STARS allows users to run standard reports for better management and tracking. However, we found inaccuracies with the reports generated. For example, the "User Allocation Report" misrepresented the total number of allocated licenses (allotted to each provider) and the actual assigned licenses (licenses in use at the provider's location). DFTA officials use this report to allocate licenses to each provider. Since PeerPlace only provides 2,150 licenses, DFTA strictly controls license allocation. As of October 2015, DFTA allocated 94 percent (2,025 licenses) of its total available licenses. However, at that time, only 1,572 licenses were actually assigned to users by the program administrators. Therefore, 22 percent (453) of allocated licenses are not being used. This misrepresentation of allocated and assigned license data may result in perceived license unavailability which may lead to user account sharing.

In addition, we found inaccuracies in the "Barcode/Bulk Unit-Event Unit Summary Report." This report allows the Senior Center staff to summarize the number of events and client attendance. However, there were inconsistencies with the report numbers. For example, the report fluctuated the count of the total number of barcode clients at the Senior Centers on a day-by-day basis. Without accurate numbers, STARS cannot be an effective management tool for program users to monitor, track, analyze, and report on clients and the services provided to them.

Inability to Delete Erroneous Event Entries

STARS lacks the ability to delete erroneous "event" entries. Senior Centers provide event services such as lunch, computer training, and painting. However, when an event is mistakenly created in STARS, it cannot be deleted, and thus poses a problem for reporting purposes. To circumvent this problem, DFTA instructed the users to change the event date to 01/01/1900 in order to exclude the event from the report. This workaround temporarily solves the report issue. However, database integrity issues could nonetheless arise over time due to the voluminous unusable data created and stored. At this time, DFTA has no standard process for properly managing and/or monitoring erroneous event entries at the provider level.

Data Validation Issues in Some Date Fields

Our tests identified data validation issues in some of the date fields within STARS. For example, dates that can only have occurred in the past can be entered with a future date, e.g., we tested "date of last physician's visit" date as 12/31/2020, a future date value and found that it was accepted by the system. Having a proper date validation function would prevent users from entering invalid past and future dates (such as 01/01/1900 or 01/01/2030), which results in incorrect client information and prevents DFTA from accurately monitoring client services. In addition, our tests found entries in the STARS' client financial and benefit fields do not automatically populate in corresponding fields throughout the online form. Thus, the information has to be re-entered. Repetitive entries increase the likelihood of data entry errors.

STARS Has Duplicate Clients

During our field visits, some program providers stated that there are duplicate client profiles in STARS. This issue was confirmed by the DFTA officials. Duplication in the client database leads to inaccuracies in monitoring and reporting client services, and may result in misappropriation of resources. Prior to creating a new client profile, STARS has a search feature that allow users to determine whether a client already exists in the database. This feature requires partial information, such as name or address to search the STARS client database. However, duplicate clients still can and do exist as a result of multiple variations of a name and/or address entered.

Although STARS has Client IDs to identify each individual, DFTA and service providers do not require the use of this ID to request services, as the 20 character Client ID is too long to expect clients' to remember. Consequently, client records may be re-created when seniors seek new services, or visit a different Senior Center and request services. This existence of multiple client records poses operational and fraud risks. It is also a concern cited by respondents on our User Satisfaction Survey.

Recommendations

DFTA should:

10. Work with PeerPlace to identify and resolve the condition that's causing unexpected user logouts.

DFTA Response: DFTA agreed with this recommendation. "DFTA was aware of this issue prior to the audit and will continue to work with the software vendor to identify the root cause(s) of these unexpected logouts and address them as they arise."

11. Ensure all reports generated by STARS are accurate and properly defined. Implement an *ad hoc* reporting feature that allows users to generate customized reports. Additionally, DFTA should periodically analyze and load balance licenses across providers for increased efficiency.

DFTA Response: DFTA generally agreed with this recommendation and stated that "While the STARS reports are accurate, DFTA will revisit the data labels used in these reports to ensure that they are clearly defined and understood. . . . DFTA tracks these licenses and their usage closely. Should a need arise to rebalance the licenses across providers in the future, DFTA will do so."

Auditor Comment: Although the agency believes that the STARS reports are accurate, our User Satisfaction Survey revealed that only 35 percent of the respondents found STARS' reports to always be accurate. Additionally, 40 percent of respondents would like to see more reporting features.

12. Work with PeerPlace to implement an event modification feature in the software, and create a policy and procedure for deleting/correcting erroneous event entries.

DFTA Response: DFTA agreed with this recommendation. "DFTA has spoken with PeerPlace, the software vendor, and this upgrade will be made."

13. Work with PeerPlace to ensure that all date fields are validated prior to accepting data entry.

DFTA Response: DFTA agreed with this recommendation. "DFTA has been working with PeerPlace to implement data validation on all date fields so that a future date cannot be entered. However, DFTA will be allowing programs to back date entries in order to accommodate their operational and staffing needs."

14. Ensure that entries in the client financial and benefit fields are stored and populated throughout the form.

DFTA Response: DFTA agreed with this recommendation. "DFTA agrees and has been aware of this need through user workgroup meetings. DFTA has recommended these changes to the State Office for the Aging, which must approve these particular changes before implementation."

15. Resolve duplicate client issues in the STARS database by using a unique, easy to remember Client ID.

DFTA Response: DFTA agreed with this recommendation. "DFTA has been tackling this problem from a myriad of approaches, including training and targeted technical assistance. From a technical viewpoint, PeerPlace has been working on developing a computerized algorithm to flag duplicates for Administrators. This feature is currently in testing and will be rolled out in the coming months."

User Satisfaction Survey

We conducted a user satisfaction survey to determine whether STARS is meeting the users' needs, and has adequate functions to ensure the information process is reliable. We distributed surveys to all 1,490 users identified as of August 10, 2015 (program providers and DFTA personnel). As of January 18, 2016, we received 663 responses (44%). In the survey, we found 78 percent of the respondents are happy or somewhat happy with the system. However, 76 percent of respondents would like to see some changes made to the system. The survey also found:

- 23% of respondents said the information displayed on the STARS screens are not easy to work with;
- 40% of respondents would like to see more reporting features; and
- 58% of respondents found the data entries to be repetitive.

In determining whether STARS has adequate functions to ensure the information process was reliable, respondents' replies include: "A lot of sections are repetitive and overly time consuming, such as the benefits and entitlements section and the financial sections." The survey also shows only 35 percent of respondents found that the reports generated by STARS were always accurate. According to one respondent, "The reports will agree with my numbers however the total is often inaccurate and needs to be recalculated on STARS' end."

DFTA provides training for new users either by classroom instruction or through online training sites. However, 19 percent of respondents felt that they require additional training. We also found that the online training site may not be up to date. Specifically, features such as upgraded edit functions were not included in the online training site.

Recommendations

DFTA should:

16. Review the design and layout of the STARS screens in order to improve readability.

DFTA Response: DFTA generally agreed with this recommendation and stated, "DFTA has an active partnership with the provider network on STARS re: system improvements and needs. DFTA will continue to enhance STARS in various ways, including changes to screen functionality, based on user input."

17. Ensure that the online training site is up to date.

DFTA Response: DFTA agreed with this recommendation. "PeerPlace will be updating the training site. DFTA will work with PeerPlace to develop a process to update the training on a regular basis."

DETAILED SCOPE AND METHODOLOGY

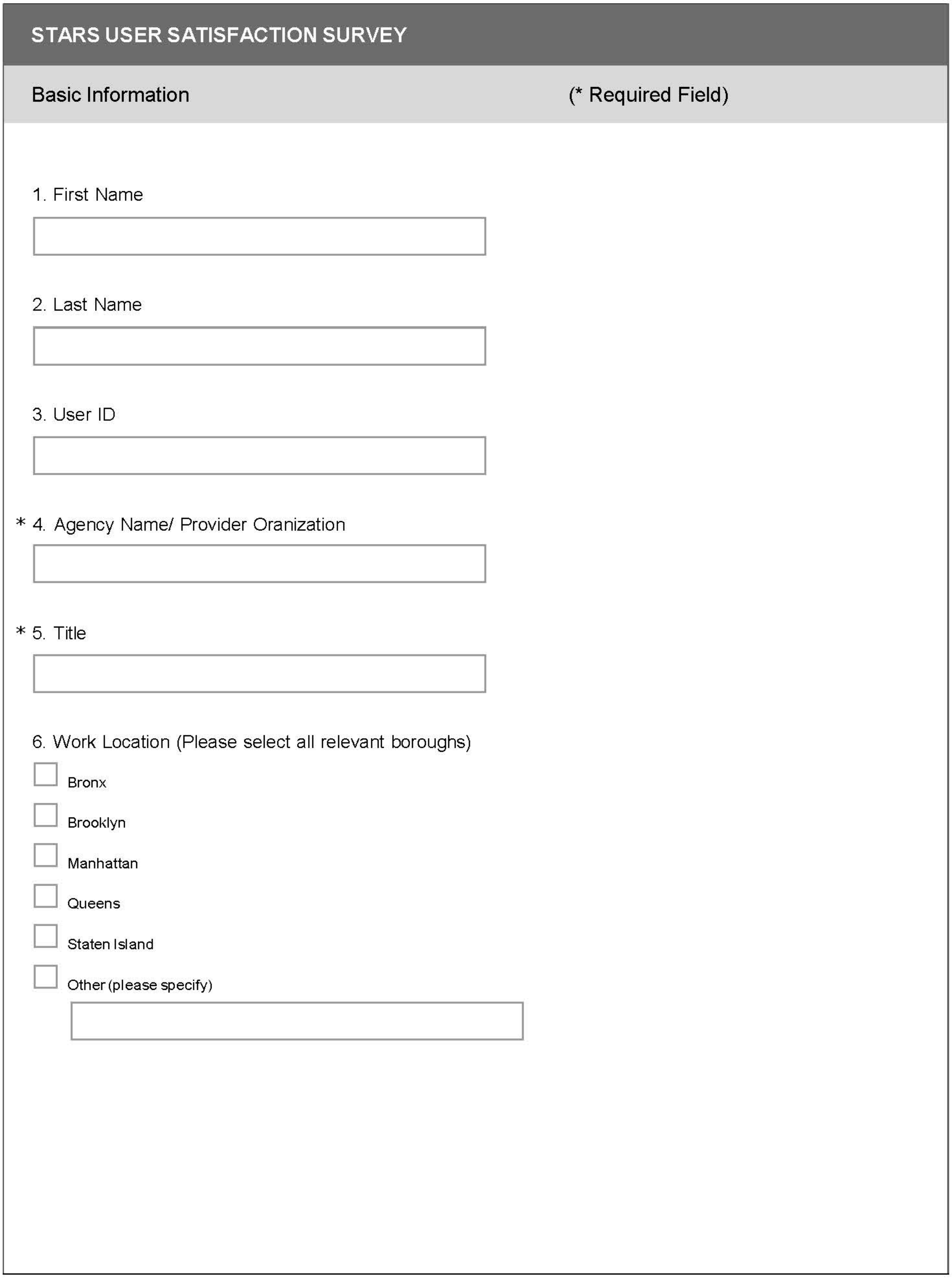
We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. This audit was conducted in accordance with the audit responsibilities of the City Comptroller as set forth in Chapter 5, §93, of the New York City Charter.

The scope of this audit was from the STARS system implementation in April 2013 to February 2016. We conducted fieldwork from October 2015 to February 2016. To achieve the audit objectives, we:

- Interviewed various DFTA officials in the following departments: Information Technology, Planning Unit, Bureau of Active Aging, Bureau of Long Term Care, Bureau of Community Services and Bureau of HealthCare;
- Reviewed the DFTA Organization Chart to gain an understanding of the administration of STARS;
- Conducted system walk-through of STARS to gain an understanding of how DFTA's and program providers' personnel performed their tasks and operations;
- Reviewed user manuals, training documents, and online video courses to gain an understanding of STARS usage and to determine whether the users were appropriately trained;
- Reviewed Comptroller's Directive #1, DoITT polices and STARS policies to determine whether adequate internal controls were present;
- Reviewed PeerPlace's contracts, amendments, and work orders to understand the project scope and contractors' responsibilities;
- Reviewed and analyzed system specifications as stated in the original Request For Proposal as a basis to determine whether system deliverables were implemented and completed on schedule;
- Reviewed and analyzed data migration mappings to verify whether DFTA had processes and procedures in place to ensure data converted from the legacy systems to the new system was accurate, complete, and successful;
- Requested and reviewed test plans and user acceptance testing sign-off documentation to determine whether DFTA had quality assurance tests in place;
- Performed system tests by creating virtual clients on the training website to determine whether STARS fulfilled the system specifications;
- Analyzed reports generated by STARS' view builder reports and other reports generated by Online Report Portal;
- Reviewed and examined user list to determine whether DFTA provided reasonable assurance to protect and secure the data from unauthorized access;
- Examined the STARS user list to determine whether DFTA users were listed as active employees on the City's Payroll Management System;

- Analyzed 68 helpdesk tickets from June to August 2015 between DFTA and PeerPlace and determined whether open items were resolved;
- Conducted field observations of 14 sites, including Senior Centers, case management, home delivery meal, home care, Naturally Occurring Retirement Community, caregiver, assigned counsel, health counseling, legal and transportation to gain understanding of the interactions between users and STARS;
- Obtained emails and newsletter from PeerPlace and DFTA to determine whether the communication channels to the users were effective;
- Reviewed PeerPlace's backup, disaster recovery and system security to determine whether PeerPlace has security controls in place to support business continuity;
- Reviewed the DFTA disaster recovery plan to determine whether DFTA has a contingency plan in place in case of an emergency; and
- Discussed with DFTA officials regarding future enhancements to address some of the current STARS shortfalls.

In addition, to determine whether STARS improved the reliability of information and if users were satisfied with the system, we conducted a User Satisfaction Survey. We received a list of 1,490 STARS users as of August 10, 2015. The survey provided users' feedback regarding STARS usability, information accuracy, sufficiency in training and effectiveness of troubleshooting.



STARS USER SATISFACTION SURVEY

Basic Information (* Required Field)

1. First Name

2. Last Name

3. User ID

* 4. Agency Name/ Provider Oranization

* 5. Title

6. Work Location (Please select all relevant boroughs)

□ Bronx

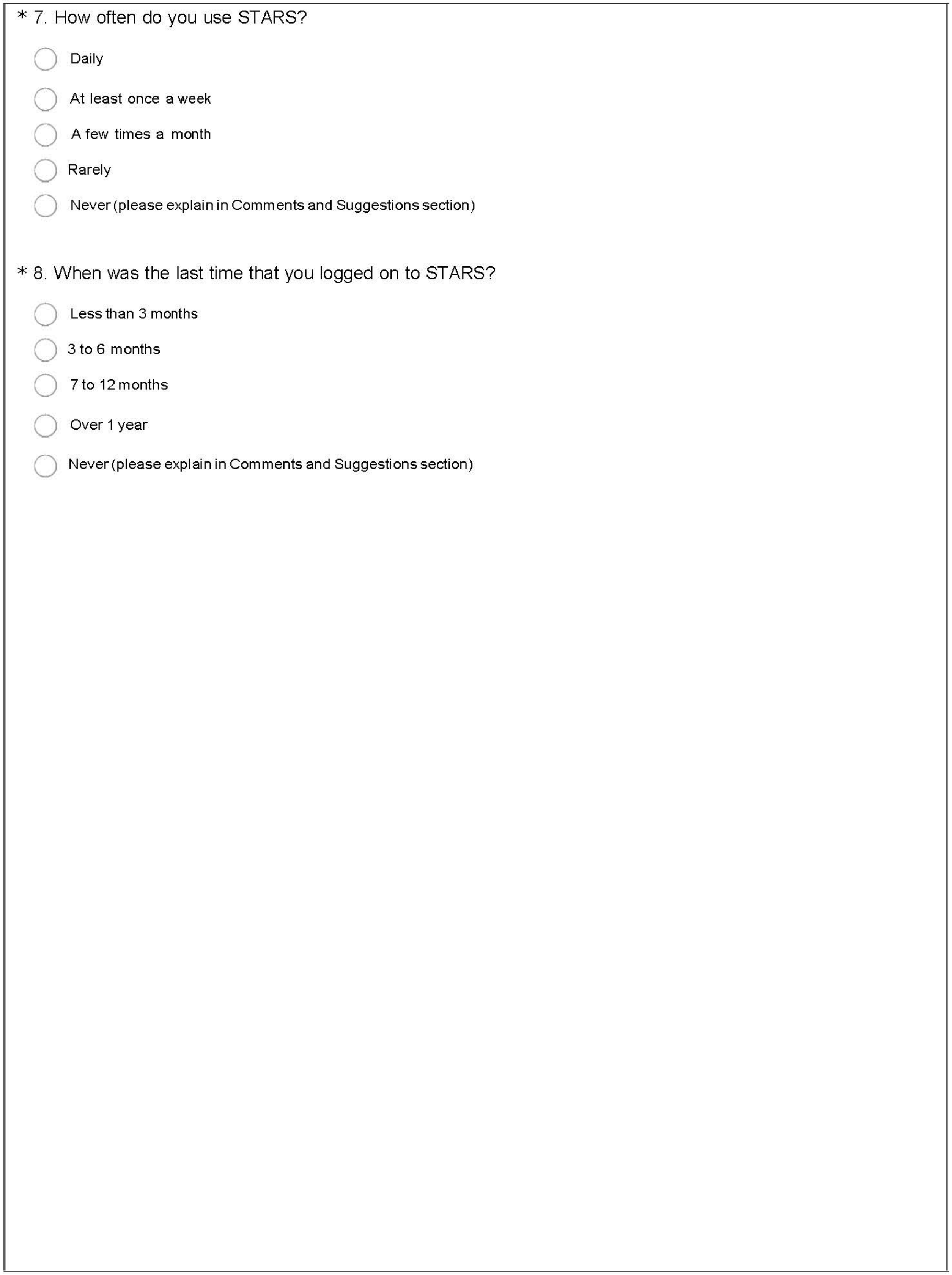
□ Brooklyn

□ Manhattan

□ Queens

□ Staten Island

□ Other (please specify)



* 7. How often do you use STARS?

○ Daily

○ At least once a week

○ A few times a month

○ Rarely

○ Never (please explain in Comments and Suggestions section)

* 8. When was the last time that you logged on to STARS?

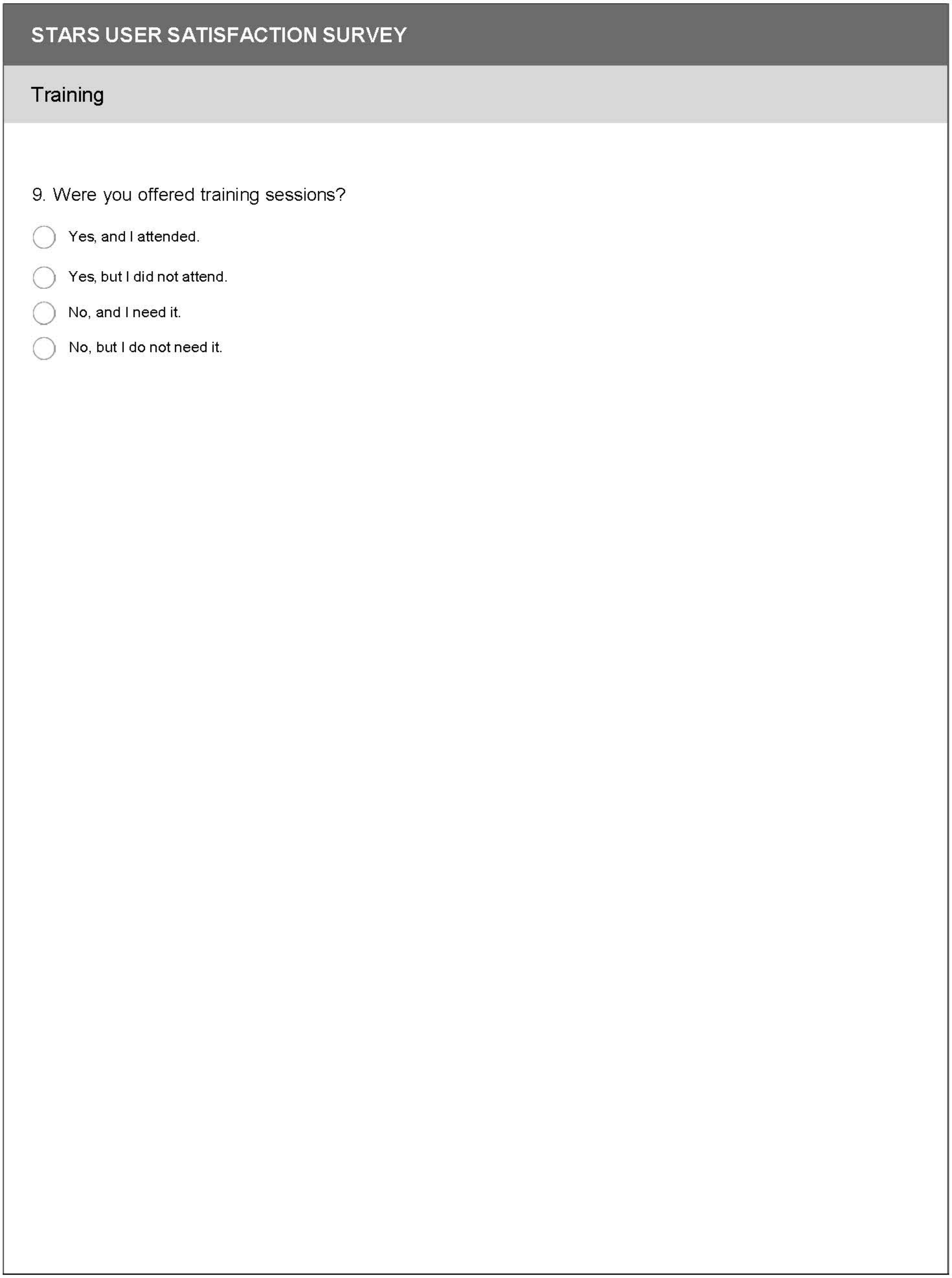
○ Less than 3 months

○ 3 to 6 months

○ 7 to 12 months

○ Over 1 year

○ Never (please explain in Comments and Suggestions section)



STARS USER SATISFACTION SURVEY

Training

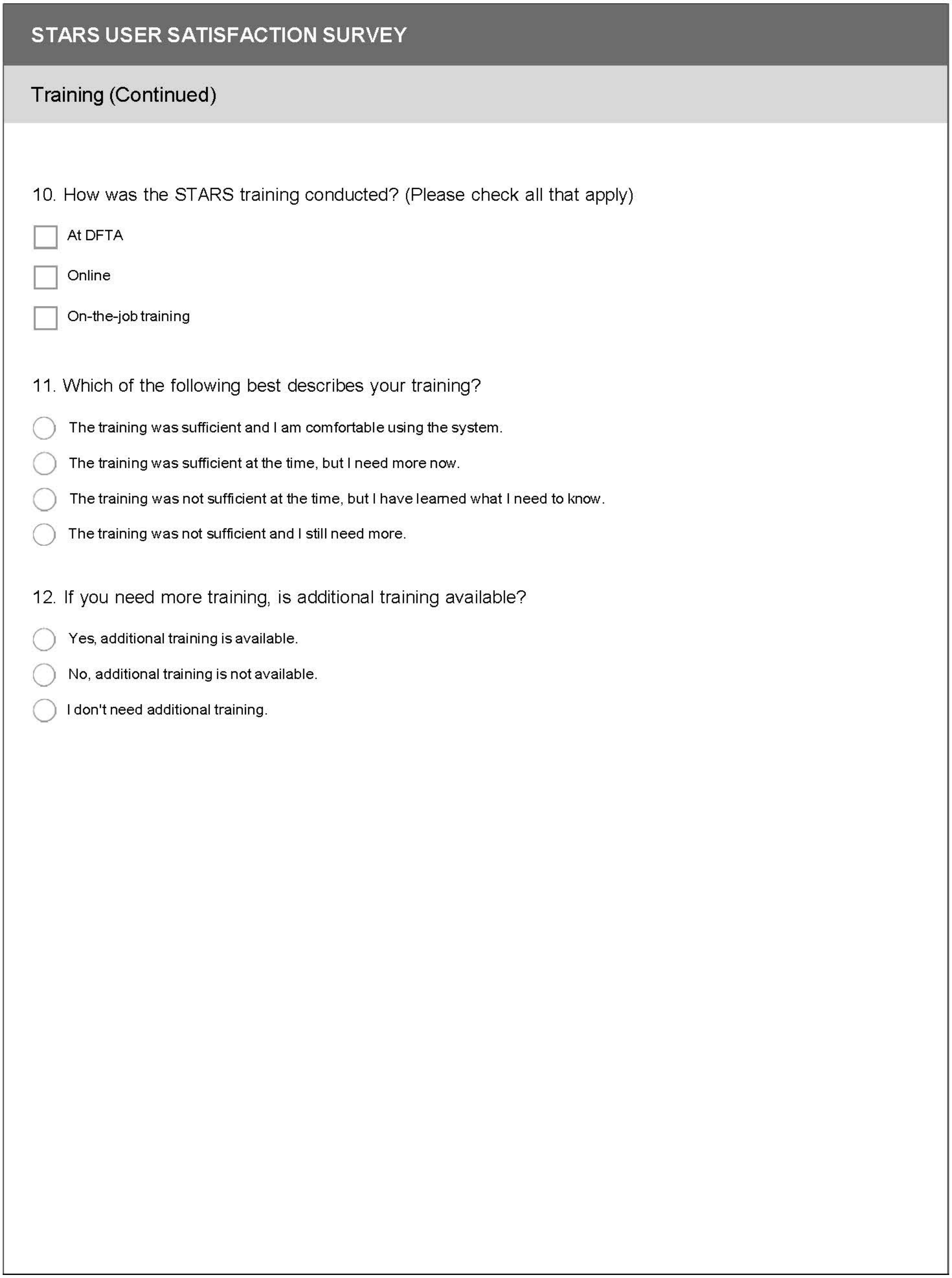
9. Were you offered training sessions?

○ Yes, and I attended.

○ Yes, but I did not attend.

○ No, and I need it.

○ No, but I do not need it.



STARS USER SATISFACTION SURVEY

Training (Continued)

10. How was the STARS training conducted? (Please check all that apply)

□ At DFTA

□ Online

□ On-the-job training

11. Which of the following best describes your training?

○ The training was sufficient and I am comfortable using the system.

○ The training was sufficient at the time, but I need more now.

○ The training was not sufficient at the time, but I have learned what I need to know.

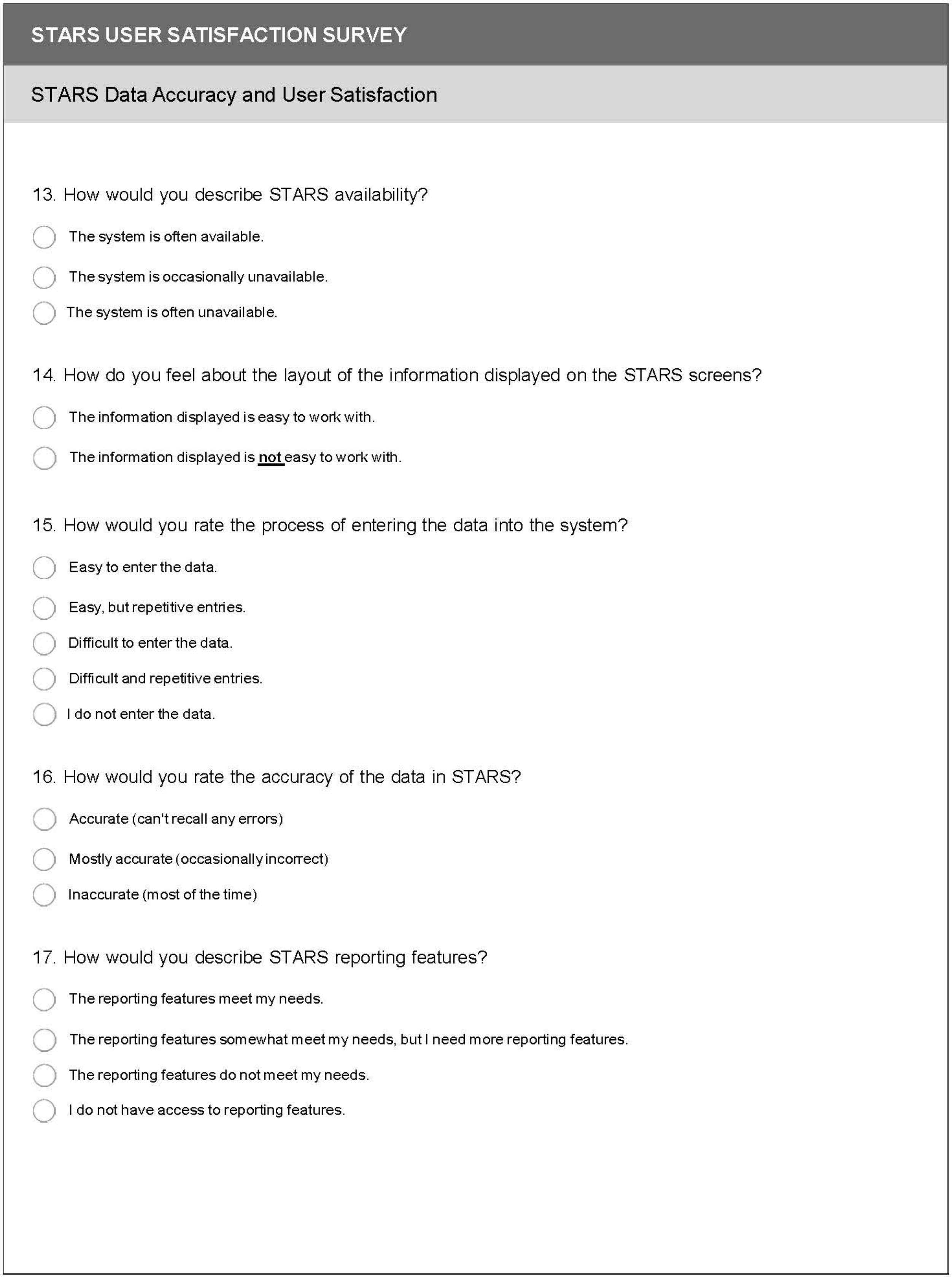
○ The training was not sufficient and I still need more.

12. If you need more training, is additional training available?

○ Yes, additional training is available.

○ No, additional training is not available.

○ I don't need additional training.



STARS USER SATISFACTION SURVEY

STARS Data Accuracy and User Satisfaction

13. How would you describe STARS availability?

○ The system is often available.

○ The system is occasionally unavailable.

○ The system is often unavailable.

14. How do you feel about the layout of the information displayed on the STARS screens?

○ The information displayed is easy to work with.

○ The information displayed is **not** easy to work with.

15. How would you rate the process of entering the data into the system?

○ Easy to enter the data.

○ Easy, but repetitive entries.

○ Difficult to enter the data.

○ Difficult and repetitive entries.

○ I do not enter the data.

16. How would you rate the accuracy of the data in STARS?

○ Accurate (can't recall any errors)

○ Mostly accurate (occasionally incorrect)

○ Inaccurate (most of the time)

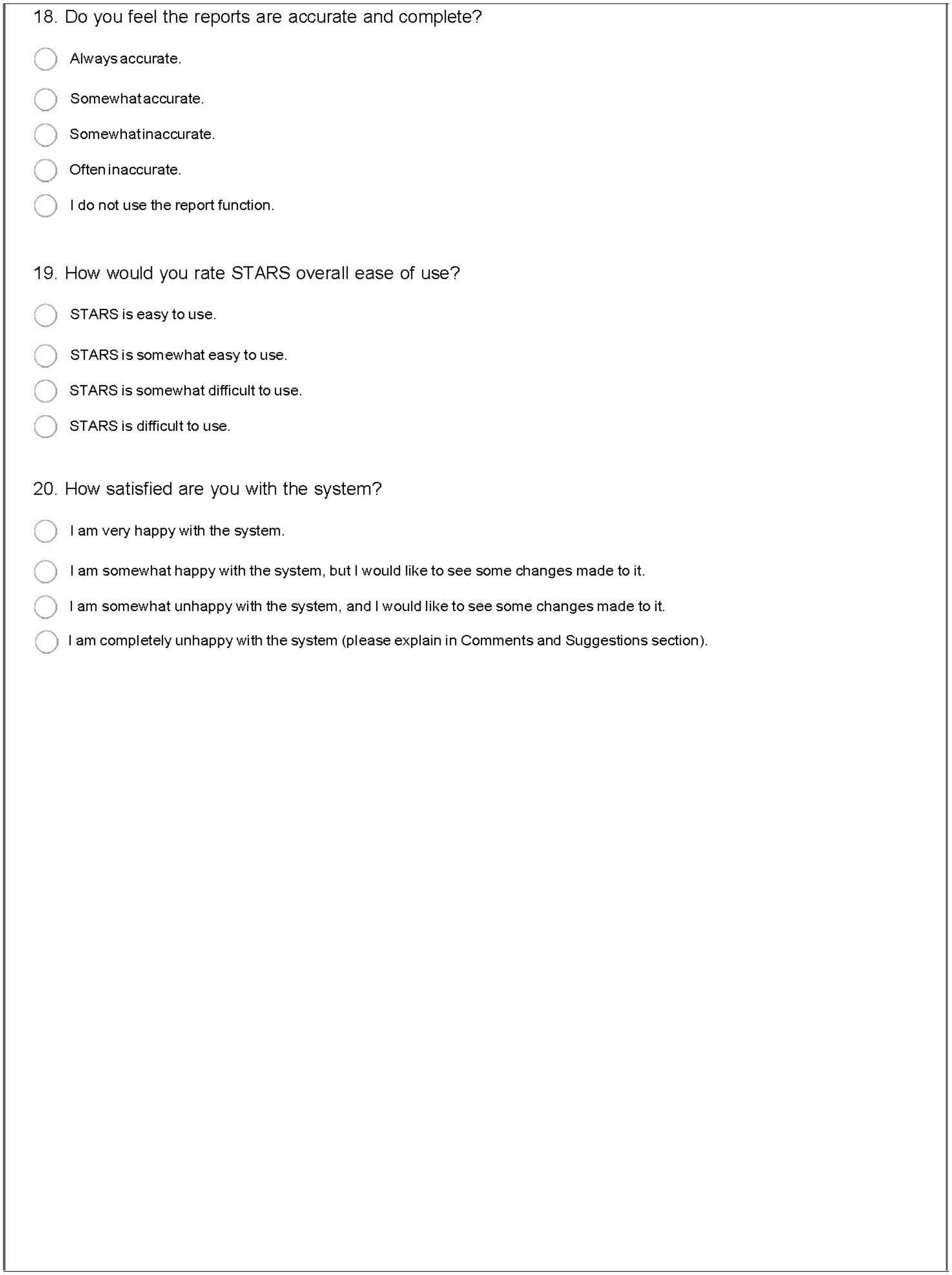
17. How would you describe STARS reporting features?

○ The reporting features meet my needs.

○ The reporting features somewhat meet my needs, but I need more reporting features.

○ The reporting features do not meet my needs.

○ I do not have access to reporting features.



18. Do you feel the reports are accurate and complete?

○ Always accurate.

○ Somewhat accurate.

○ Somewhat inaccurate.

○ Often inaccurate.

○ I do not use the report function.

19. How would you rate STARS overall ease of use?

○ STARS is easy to use.

○ STARS is somewhat easy to use.

○ STARS is somewhat difficult to use.

○ STARS is difficult to use.

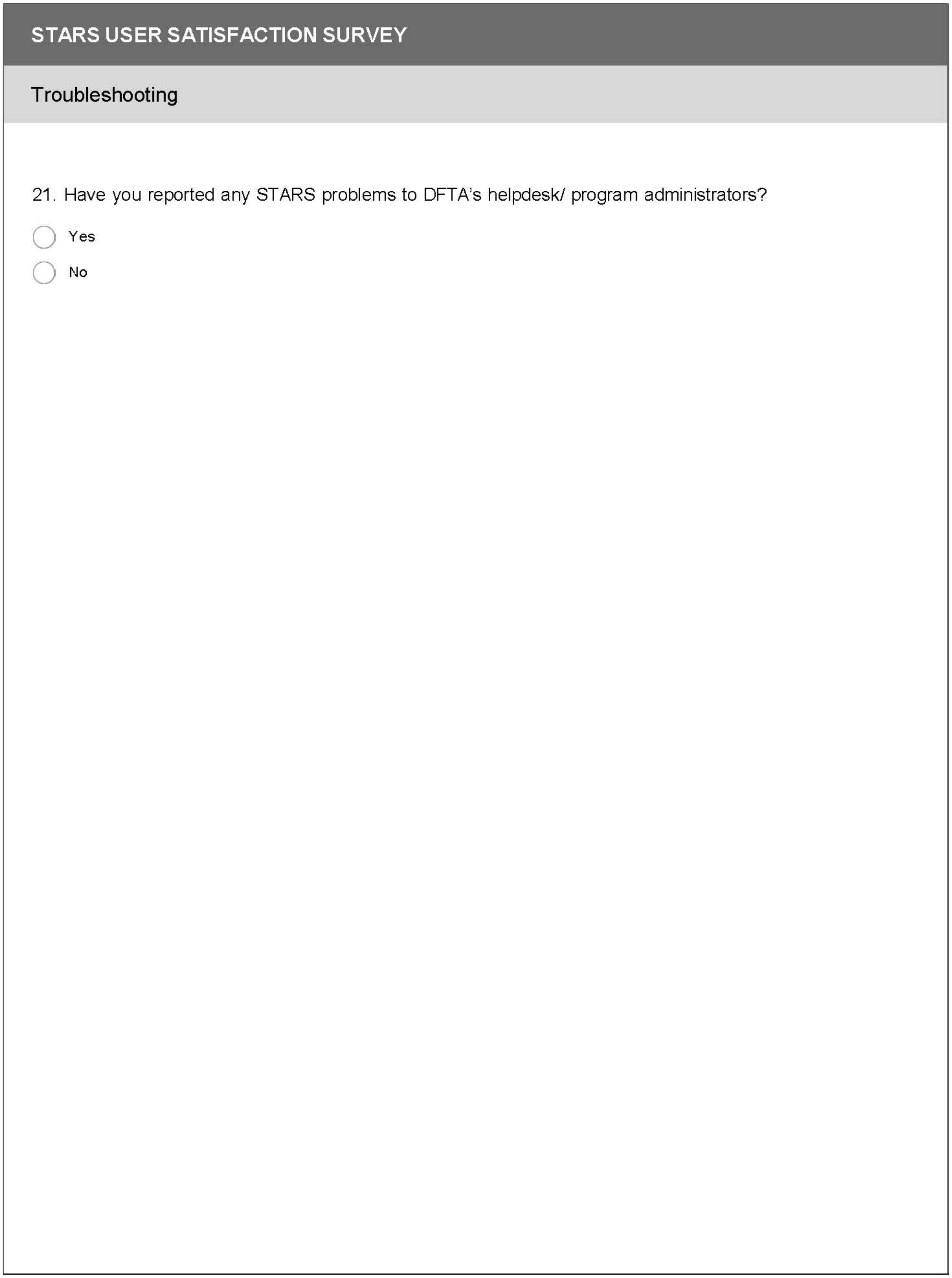
20. How satisfied are you with the system?

○ I am very happy with the system.

○ I am somewhat happy with the system, but I would like to see some changes made to it.

○ I am somewhat unhappy with the system, and I would like to see some changes made to it.

○ I am completely unhappy with the system (please explain in Comments and Suggestions section).



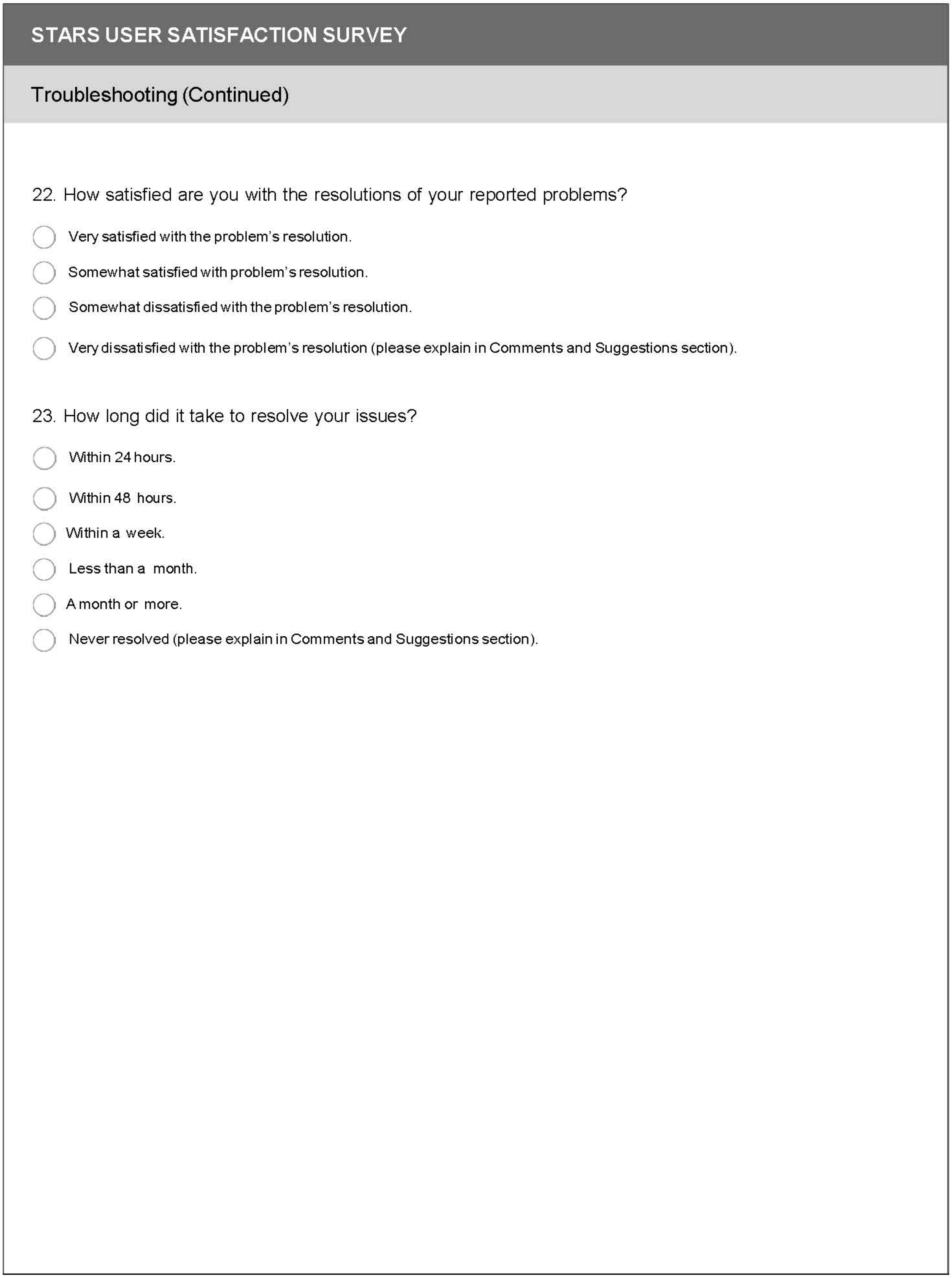
STARS USER SATISFACTION SURVEY

Troubleshooting

21. Have you reported any STARS problems to DFTA's helpdesk/ program administrators?

○ Yes

○ No



STARS USER SATISFACTION SURVEY

Troubleshooting (Continued)

22. How satisfied are you with the resolutions of your reported problems?

○ Very satisfied with the problem’s resolution.

○ Somewhat satisfied with problem’s resolution.

○ Somewhat dissatisfied with the problem’s resolution.

○ Very dissatisfied with the problem’s resolution (please explain in Comments and Suggestions section).

23. How long did it take to resolve your issues?

○ Within 24 hours.

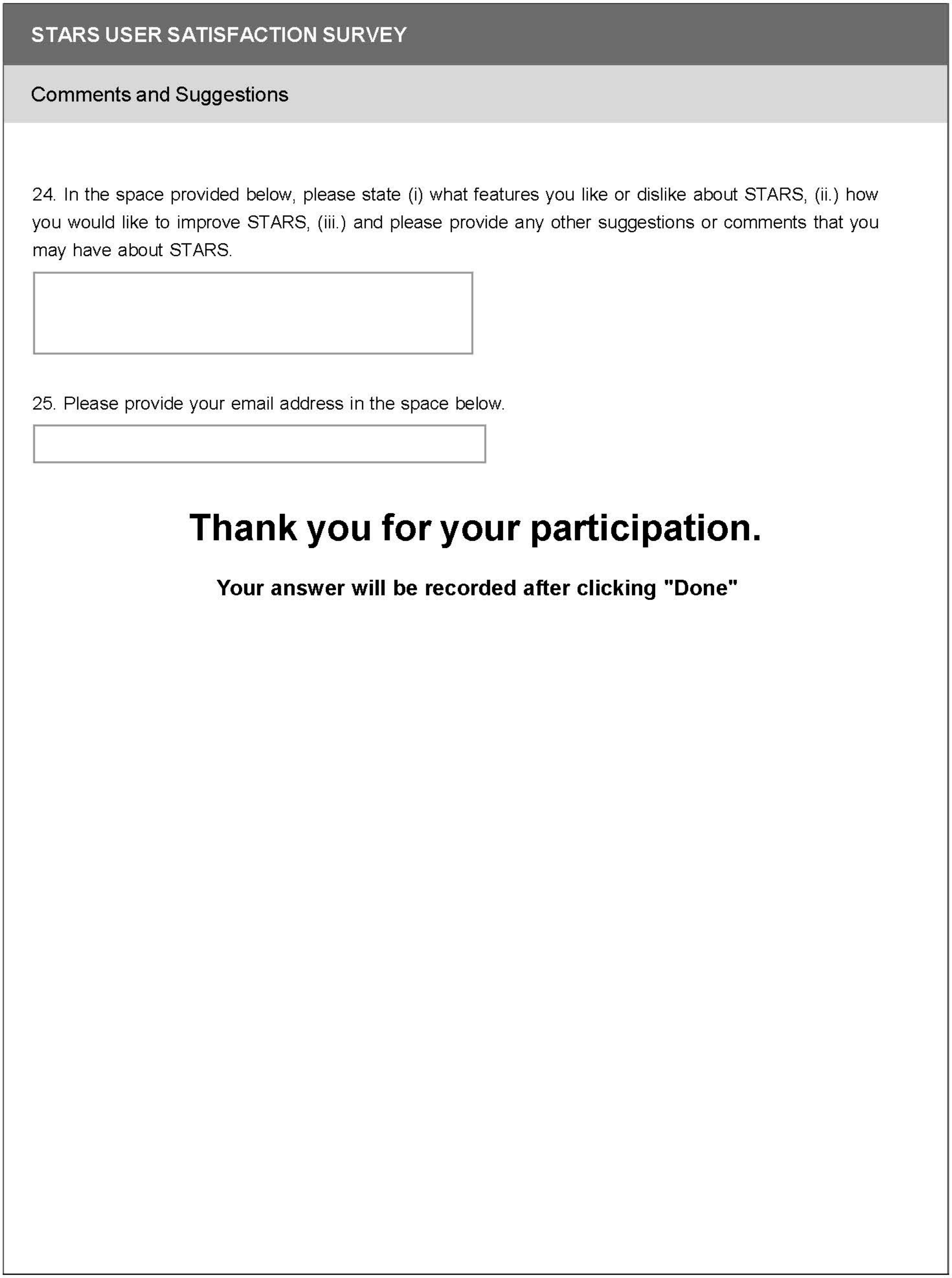
○ Within 48 hours.

○ Within a week.

○ Less than a month.

○ A month or more.

○ Never resolved (please explain in Comments and Suggestions section).



STARS USER SATISFACTION SURVEY

Comments and Suggestions

24. In the space provided below, please state (i) what features you like or dislike about STARS, (ii.) how you would like to improve STARS, (iii.) and please provide any other suggestions or comments that you may have about STARS.

25. Please provide your email address in the space below.

Thank you for your participation.

Your answer will be recorded after clicking "Done"

Department for the Aging

Donna M. Corrado, PhD
Commissioner

2 Lafayette St. 7th Fl
New York, NY 10007

212 602 4100 tel
212 442 1095 fax

June 15, 2016

Marjorie Landa
Deputy Comptroller for Audit
Office of the Comptroller
One Centre Street, Room 1100
New York, NY 10007-2341

Re: Comptroller's Audit Report on the Development and Implementation of the Senior Tracking, Analysis and Reporting System (STARS) Administered by the Department for the Aging (SI15-121A)

Dear Deputy Comptroller Landa:

Thank you for the opportunity to respond to your June 2, 2016 "Audit Report on the Development and Implementation of the Senior Tracking, Analysis and Reporting System (STARS) Administered by the Department for the Aging (DFTA)."

DFTA has reviewed the audit report, and we are pleased to see that the Comptroller's independent survey found that 78% of users said the system is very or somewhat useful. This is especially encouraging given that DFTA oversees more than 500 direct service contracts covering 12 different programs.

DFTA is also pleased that the auditors independently conclude that "...the overall goals of STARS as stated in the system specifications have generally been met." STARS was implemented in 2013, and its impact was far-reaching. STARS' success is attributable to DFTA's modus operandi of regularly seeking providers' input about the system, which was extensive, and ensuring that their needs are accommodated through STARS.

DFTA is always looking to do better and improve on what we have. We would like to thank the Comptroller's auditors for their time, thoroughness and recommendations. DFTA will be following up on them. Please see below for further details.

*****

Audit Recommendation #1: Ensure any future contract changes are made in full compliance with the PPB rules.

DFTA Response: From the time of the release of the STARS solicitation to the selection of the software vendor, three program modules that were included in the original solicitation were no longer needed. STARS is a multi-million dollar IT project, which included funding for those three modules, which amounted to $36,054.

So, DFTA redirected those dollars for other enhancements in STARS in response to providers' needs. These monies were accounted for and tracked through work orders. Every invoice was signed off and accounted for by the project manager. The competitive hourly rate remained the same as the RFP rate, and the contract value stayed the same, i.e. these work orders did not change the contract amount. Supporting documentation of the work orders, the invoices and the wage rate have been shared with the auditors. The funds were never at risk of financial mismanagement.

With that said, DFTA recognizes that contract changes need to be formally memorialized through the City's change order process. The Department will be mindful of doing so in the future.

*****

Audit Recommendation #2, #3: Ensure that STARS complies with DoITT's Citywide Security Policies and Standards. Ensure all future system developments and enhancements are made in accordance with DoITT policies.

DFTA Response: DFTA has contacted DoITT's Citywide Chief Information Security Officer (CCISO), who oversees the Citywide Cybersecurity Program, for guidance. DFTA and the Cybersecurity Program will evaluate the cybersecurity hygiene of STARS to determine if additional steps need to be taken. DFTA will be scheduling a follow-up meeting with DoITT in a few weeks for further discussion.

DoITT's Service Catalog outlines the IT Security accreditation needed for cloud-based systems such as STARS. PeerPlace, the company that developed the STARS system already has a SOC2-Type II accreditation which is recognized by DoITT. Furthermore, this client tracking software is now mandated by the State Office for the Aging and will be used by all 59 Area Agencies on Aging in New York State.

*****

Audit Recommendation #4: Require STARS users to comply with DoITT's Password policy.

DFTA Response: DFTA agrees. PeerPlace will implement an automatic 90-day password expiration where the same password cannot be reused for four or more iterations.

*****

Audit Recommendation #5: Enforce Access Protocols regarding users sharing accounts, and periodically perform assessments to ensure users comply with appropriate access controls.

DFTA Response: DFTA agrees. Commencing prior to this audit, DFTA has been working on a STARS Program Administrators Guide. This Guide will reiterate DFTA's STARS' Usage Policy and strict prohibition on sharing user names and passwords. DFTA will post this Guide directly on STARS for user access. DFTA will also be including the STARS usage policy in program standards as part of the assessment.

*****

Audit Recommendation #6: Notify all service providers of the Access Protocols, and instruct the providers to: (1) discontinue the practice of setting user accounts with the same password immediately; and (2) discontinue the practice of allowing multiple users to share the same email address immediately.

DFTA Response: DFTA agrees. This recommendation will be incorporated into DFTA's STARS Usage Policy. Instructions to providers will be drafted and released immediately. DFTA is currently working on implementing this recommendation.

Audit Recommendation #7: Ensure all terminated or inactive employee accounts are deactivated from STARS immediately.

DFTA Response: DFTA agrees, and this recommendation is in line with DFTA's current STARS Usage Policy. DFTA will reiterate to providers the security risks that are posed when former employees are not immediately inactivated from STARS. DFTA currently has a 45-day auto-inactivation in the STARS system. DFTA will be reducing this inactivation period to 15 days.

*****

Audit Recommendation #8: Review all accounts and ensure that STARS users are granted the minimum level of privileges necessary for them to perform their job functions.

DFTA Response: DFTA agrees. DFTA will incorporate this recommendation into the DFTA STARS Usage Policy. Instructions to providers will be drafted and released immediately.

*****

Audit Recommendation #9: Restrict STARS administrators' access to their assigned jurisdiction only.

DFTA Response: DFTA agrees. Prior to this audit, DFTA recognized that this restriction is needed. DFTA has been working with the software vendor on this restriction.

*****

Audit Recommendation #10: Work with PeerPlace to identify and resolve the condition that's causing unexpected user logouts.

DFTA Response: DFTA agrees. DFTA was aware of this issue prior to the audit and will continue to work with the software vendor to identify the root cause(s) of these unexpected logouts and address them as they arise.

*****

Audit Recommendation #11: Ensure all reports generated by STARS are accurate and properly defined. Implement an *ad hoc* reporting feature that allows users to generate customized reports. Additionally, DFTA should periodically analyze and load balance licenses across providers for increased efficiency.

DFTA Response: While the STARS reports are accurate, DFTA will revisit the data labels used in these reports to ensure that they are clearly defined and understood.

There is currently a wealth of canned reports (109) available to DFTA staff and providers through STARS. These canned reports were created based on conversations with providers and their needs, and where a particular need arises for a customized report, DFTA IT's staff have been able to create them for individual providers. DFTA will reach out to the software provider to see if developing an *ad hoc* reporting feature is feasible and fiscally prudent.

Re: licensing, DFTA allocates licenses based on anticipated program needs so programs do not have to come back to DFTA constantly for additional users. DFTA tracks these licenses and their usage closely. Should a need arise to rebalance the licenses across providers in the future, DFTA will do so.

Audit Recommendation #12: Work with PeerPlace to implement an event modification feature in the software, and create a policy and procedure for deleting/correcting erroneous event entries.

DFTA Response: DFTA agrees. DFTA has spoken with PeerPlace, the software vendor, and this upgrade will be made.

*****

Audit Recommendation #13: Work with PeerPlace to ensure that all date fields are validated prior to accepting data entry.

DFTA Response: DFTA agrees and has been working on this date validation prior to the audit. DFTA has been working with PeerPlace to implement data validation on all date fields so that a future date cannot be entered. However, DFTA will be allowing programs to back date entries in order to accommodate their operational and staffing needs.

*****

Recommendation #14: Ensure that entries in the client financial and benefit fields are stored and populated throughout the form.

DFTA Response: DFTA agrees and has been aware of this need through user workgroup meetings. DFTA has recommended these changes to the State Office for the Aging, which must approve these particular changes before implementation.

*****

Audit Recommendation #15: Resolve duplicate client issues in the STARS database by using a unique, easy to remember Client ID.

DFTA Response: DFTA agrees. Addressing this human error issue has been a priority for DFTA even prior to the audit. DFTA has been tackling this problem from a myriad of approaches, including training and targeted technical assistance. From a technical viewpoint, PeerPlace has been working on developing a computerized algorithm to flag duplicates for Administrators. This feature is currently in testing and will be rolled out in the coming months.

*****

Audit Recommendation #16: Review the design and layout of the STARS screens in order to improve readability.

DFTA Response: DFTA has an active partnership with the provider network on STARS re: system improvements and needs. DFTA will continue to enhance STARS in various ways, including changes to screen functionality, based on user input.

*****

Audit Recommendation #17: Ensure that the online training site is up to date.

DFTA Response: DFTA agrees. PeerPlace will be updating the training site. DFTA will work with PeerPlace to develop a process to update the training site on a regular basis.

The Department would like to thank the Comptroller's office for the helpful recommendations in this audit. DFTA will be following up on these recommendations as it continues its ongoing work to further enhance and improve STARS functionality.

If you have any questions about our reply, please contact John Jones at (212) 602-4495 or by e-mail at jjones@aging.nyc.gov.

Sincerely,

Donna M. Corrado
Commissioner

cc: Michael Bosnick, DFTA
Steven Foo, DFTA
John Jones, DFTA
Joy Wang, DFTA
Mindy Tarlow, Mayor's Office of Operations
George Davis, III, Mayor's Office of Operations