NJ-2017-002

Contractor Supplied Device Survey

FINAL REPORT
July 2017

Submitted by

Chris Titze
Christian Higgins
Cambridge Systematics, Inc.
New York, New York 10016

NJDOT Research Project Manager
Camille Crichton-Sumners

In cooperation with

New Jersey
Department of Transportation
Bureau of Research

DISCLAIMER STATEMENT

“The contents of this report reflect the views of the authors who are responsible for the facts and the accuracy of the data presented herein. The contents do not necessarily reflect the official views or policies of the New Jersey Department of Transportation. This report does not constitute a standard, specification, or regulation.”

TECHNICAL REPORT
STANDARD TITLE PAGE

1. Report No. NJ-2017-002	2. Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle Contractor Supplied Device Survey FINAL REPORT		5. Report Date July 2017 6. Performing Organization Code
7. Author(s) Titze, Chris; Higgins, Christian		8. Performing Organization Report No.
9. Performing Organization Name and Address Cambridge Systematics, Inc. 38 East 32nd Street, 7th Floor New York, NY 10016		10. Work Unit No. 11. Contract or Grant No.
12. Sponsoring Agency Name and Address New Jersey Department of Transportation P.O. 600 Trenton, NJ 08625		13. Type of Report and Period Covered: Final Report (not covered) 14. Sponsoring Agency Code
15. Supplementary Notes		

16. Abstract

Contractor supplied devices (CSDs) play an important role in the day-to-day operations of NJDOT staff. Consisting of multiple devices used in office and field settings, CSDs are used at all stages of NJDOT projects and operations. Given a limited supply of devices and technology to cover a range of statewide projects and operations, reliance, to a certain extent, on contractors to supply this equipment is a necessity. The fact that these devices are owned by independent contractors however, presents multiple complexities regarding how data, used for NJDOT purposes is managed, as well how these devices are managed and allocated. The purpose of this document is to better understand best practices in CSDs are managed by other State DOTs, as well as how CSDs are utilized by NJDOT staff.

17. Key Words Contractor supplied device; security, data, information, management	18. Distribution Statement

19. Security Classif. (of this report) Unclassified	20. Security Classif. (of this page) Unclassified	21. 53 pages	22. Price

Form DOT F 1700.7 (8-69)

ACKNOWLEDGEMENTS

The authors of this report wish to thank the staff from the New Jersey Department of Transportation's (NJDOT) Bureau of Research of without whom completion of this report would not have been possible. In addition, the authors would like to thank the Virginia Department of Transportation (VDOT), Ohio Department of Transportation (ODOT), New York Department of Transportation (NYSDOT), Florida Department of Transportation (FSDOT), Georgia Department of Transportation (GDOT), Oregon Department of Transportation (ODOT) and San Jose Department of Transportation for making themselves available to the authors and sharing their experiences.

TABLE OF CONTENTS

List of Figures **Page**

List of Tables **Page**

EXECUTIVE SUMMARY

The New Jersey Department of Transportation (NJDOT) Bureau of Research is in the process of developing an appropriate policy to govern the use of contractor-supplied devices and equipment (CSDs). Through this research, NJDOT sought to determine how CSDs are managed in other states, as well as how they are used by NJDOT staff in the workspace.

NJDOT contracted with Cambridge Systematics, Inc. (the "Research Team") to research administrative contractual provisions used by other states to manage CSD hardware and software, and to develop and deploy a web-based survey on CSDs to be disseminated to NJDOT staff.

The Research Team conducted a literature review, developed and conducted an interview with other State DOTs and developed, field-tested and deployed a web-based survey to NJDOT staff to assist NJDOT in improving its CSD management procedures.

Research Questions

This research effort was guided by the following key questions:

Where and how are contractor supplied devices (CSDs) deployed and what contractual mechanisms and procedures are used to manage the acquisition, deployment and post-project disposition of CSDs?

CSDs are utilized throughout the NJDOT workspace, including within headquarters, regional and field offices. This appears to be the case at NJDOT, as well as throughout the other state DOTs. The use of CSDs throughout these workspaces is attributed to the different types of CSDs which are employed. The exception to this was Ohio Department of Transportation (ODOT), which does not employ very many CSDs. Instead, they run preliminary pilot projects to determine the necessary hardware and then acquire it on their own whenever possible. Within NJDOT, surveying results revealed that CSDs are likely more prevalent and take the form of computers, phones and other workspace devices such as printers and fax machines.

While CSDs are usually treated at a different security level than those DOT-supplied devices, the contractual mechanisms and procedures used to manage the acquisition, deployment and post-project disposition of CSDs vary. The most stringent contract mechanisms are deployed by ODOT as a result of previous negative experiences with vendors that suddenly stopped work. Although it can be difficult to determine liability, ODOT places blame on the contractors if the devices used to collect and manage data were functioning properly, but the actual data collection process is faulty. In such cases where the blame is proven to fall on the contractors, they are given a total of 30 days to remediate the issue, before additional steps are taken.

An additional trend is the use of different districts within the NJDOT to manage device inventory, including CSD needs. In this means of management, devices can be shared

and borrowed amongst the different districts. This format works particularly well for construction needs, but does can lead to inconsistency issues in terms of IT data collection. NJDOT currently does not employ this strategy, with devices being managed instead at the headquarters level.

How are CSDs used by NJDOT staff to collect, manage and share information related to NJDOT projects and contracts?

The use of CSDs to collect, manage and share information on the part of NJDOT staff varies based on the device being used. More often than not, NJDOT staff are responsible for managing information stored on CSDs. This was reflected in the survey results which indicated that over half of respondents are responsible. In addition to other employees and vendors, an additional popular result regarding this theme was that information is not actually transferred to another storage device or location, but rather remains on the CSD. A surprisingly less popular answer from the survey was that CSD-collected and managed information syncs with a server or other cloud-based system automatically. This may be attributed to the standard level of VPN access given to contractors by the NJDOT. In a review of existing policies on the part of other State DOTs, VPN access varied noticeably, with some states actually excluding contractors and vendors from any of such access.

When asked about the frequency that staff share and upload information from CSDs, there was a lot more uncertainty. Approximately 75% of respondents reported that they were not sure and/ or didn't keep track. The second most popular response was only as needed during the project, with the responses not varying based on who and how the information is actually shared and uploaded.

What data and information reside on CSDs?

Data and information residing on CSDs is dependent on the type of CSD being utilized. Results of the survey indicated that a wide variety of devices constitute CSDs including computers, phones and other workspace devices. As a result, data and information residing on CSDs will vary by project and task, but is likely involved in all levels of the project development, planning, implementation and evaluation process.

How are data and information transmitted between the CSDs and NJDOT-controlled information systems and file servers while a project is in progress?

Based on the survey results, it was found that data transferring between CSDs and NJDOT devices does not occur frequently. In fact, over half of all survey respondents indicated that they do not actually move data between CSDs and NJDOT devices. Those respondents that do transfer data between the two types of devices tend to use thumb drives, or email, which tended to be the most common response. Additional methods of data transferring between the two types of devices included the use of a VPN, personal PC and CD or DVD burning. However, these additional methods are much less commonly used.

The variety in methods used to transmit data between CSDs and DOT-controlled information systems is further reflected in national trends. The use of email as a means of transmitting data is also a primary means for the Maryland Department of Transportation (MDOT), though MDOT also uses software packages when files become particularly large. Although Kansas Department of Transportation (KDOT) typically uses a VPN for these purposes, MDOT and North Carolina Department of Transportation (NCDOT) do not allow contractor devices to connect to VPNs. Additionally, although the use of CD and DVD burning to transmit information is less common within NJDOT, it is employed as a primary method by ODOT. These results indicate that there is currently no universally accepted method of uploading information between the two types of devices.

How are (and is) data and information stored on CSDs transmitted to and archived by NJDOT during the project close out process?

Note: None of the survey questions directly addressed this. Will leave this question open for further discussion with Chris/Brian.

Key Research Conclusions

CSDs are Necessary in the NJDOT Workspace

The use of CSDs is necessary in the NJDOT workspace as staff utilize these devices in the same ways that they utilize NJDOT-supplied devices. This can be attributed to limited supply and functionality of DOT-owned devices and the associated capital investments that would be needed to maintain an adequate supply. As a result, when managed properly, CSD use can be seen as a money-saving tactic.

Policies Governing Use and Management of CSDs Vary

Across other State DOTs, policies regarding the use and management of CSDs vary noticeably. For example, certain State DOTs prohibit VPN access to contractors and vendors, while other State DOTs allow this. There currently isn't a standardized best practices and recommendation guide for State DOTs to follow regarding CSDs.

Staff Does Not Have a Preference for CSDs over DOT-Supplied Devices

NJDOT staff do not have a preference for whether devices are supplied by NJDOT or a contractor. In those instances where NJDOT staff indicated that they had a preference for CSDs, it was attributed to the NJDOT not actually supporting or providing that type of device. If those devices were in fact supported or provided by NJDOT, staff would not have any issues using those devices.

BACKGROUND

CSDs play an important role in the day-to-day operations of NJDOT staff. Consisting of multiple devices used in office and field settings, CSDs are used at all stages of NJDOT projects and operations. Given a limited supply of devices and technology to cover a

range of statewide projects and operations, reliance, to a certain extent, on contractors to supply this equipment is a necessity. The fact that these devices are owned by independent contractors however, presents multiple complexities regarding how data, used for NJDOT purposes is managed, as well how these devices are managed and allocated. The purpose of this document is to better understand best practices in CSDs are managed by other State DOTs, as well as how CSDs are utilized by NJDOT staff.

OBJECTIVES

The goal of this research was to provide NJDOT with a comprehensive understanding of the following elements regarding CSDs:

- Best practices regarding state DOT management of CSDs, including administrative procedures and contractual mechanisms
- How information on CSDs managed and securely stored
- How information transmitted between CSDs and in-house information management systems and file servers
- Where and how are CSDs used by NJDOT staff
- How (and is) data and information stored on CSDs transmitted to and archived by NJDOT during the project closeout process

INTRODUCTION

The performed research was designed to provide the NJDOT Bureau of Research with a better understanding of how contractor supplied devices (CSDs) are deployed and what contractual mechanisms and procedures are used to manage the acquisition, deployment, and post-project disposition of CSDs. This includes how CSDs are utilized in the workspace to collect, manage and store different kinds of data, as well as how that data is transmitted to and from NJDOT-controlled information systems and file servers. In addition to this information, the report provides recommendations on what the NJDOT should do to improve its CSD management procedures and related information management procedures.

SUMMARY OF THE LITERATURE REVIEW

The research team performed a literature and best practices review of existing policies and procedures that govern how state DOTs manage CSDs, from the basic use of devices to data management and contractor liability. Those policies and procedures are summarized and detailed in the following categories:

Security Best Practices

Key security best practices govern the following:

VPN Access

In order to maintain secure networks, DOTs grant third party contractor's network access through VPNs so that their access is restricted to exactly what software and programs they need. To accomplish this the DOT can provide a hosted, offsite solution that uses the network in a limited way with access to whatever software the job requires. In this environment, the network and portals are more crucial than the devices themselves.

Enforcement of Security Policies, Including Updated Anti-Virus Software

Another security measure is to ensure that contractors have installed, maintained and operate anti-virus software on any device that accesses a DOT network.

Contracting and Project Close-Out Procedures

In addition to how devices are used during a project, as defined in a contract, project close-out procedures are also important: DOTs should ensure that all media (hard drives, disks, hardware, etc.) used by contractors that contain DOT information must be returned to that DOT for sanitization or destruction.

Pass-Through of Security Provisions to Subcontractors

Lastly, whether the third party is a contractor or a university, the same security scrutiny should apply to all third parties.

Efficiency of Work Flows and Data Transfers

After security, another important factor is device usability so that third parties can properly and efficiently perform the work they need to. Ultimately, this is more important than if the contractor uses their own device or a DOT-supplied device. Different states handle this differently, where some states build new networks that lie between the guest network and production network for contractors to have limited access, while other states supply all equipment for contractor use. Cost effectiveness may be the deciding factor between the two options. That said, if the equipment is DOT-owned, it can be configured more quickly to ensure security and it reduces the variables involved with CSDs.

Device Availability and Troubleshooting

All of these measures are important and assume that hardware, software and systems function properly; when they don't, contractors provide their own technical and financial support if the problem is their hardware, though if the VPN is at fault then the DOT must resolve it. However, given these complex interfaces, sometimes it can be difficult to discern the root of the problem. The best practices in holding contractors liable for hardware, software, training and related deliverables is to give them 30 days to correct the problem and if uncorrected after that time, to resolve it through adjudication.

Data Access and Ownership

Data access and ownership is a concern for many DOTs. While most DOTs own the data that they pay contractors to collect, unfettered data access is equally acceptable to data ownership. Data collection and transmission varies depending on the type of equipment that is used and its relationship to the network; all of the following are possible: automatic collection and transmission, transmission via a VPN, transmission by directly tapping into the hardware. For most mobile equipment, the data is transitory to the device because it automatically transmits the collected data once connected to the network; this data transmit into a repository, where it is cleansed, then automatically transmitted to a DOT database, or it is manually fetched from the repository. Data backup may occur automatically or via a vendor that provides this services.

Policies and Procedures to Promote Standardization

Lastly, some DOTs manage their device inventory in silos, where each functional area or division manages their devices according to their own procedures, while headquarters makes recommendations and shares best practices. This decentralized management structure can result in lack of inventory control and data consistency problems. For example, because districts dictate their own policies, three different districts may collect the same information but may input “Street”, “St” or “St.” Because of this it is recommended that policies, procedures and inventory be centralized.

SUMMARY OF WORKED PERFORMED

The research team divided the work effort into three tasks, as follows:

1. Review of Best Practices
2. Develop and Field Test Survey
3. Deploy and Analyze Survey

The following sections of this report include detailed analyses of each category.

Task 1 - Comparative Analysis

The research team began with a review of administrative procedures and contractual provisions used by other states to manage CSD hardware and software as well as information that resides on the CSDs.

Policies and Procedures Governing Use of CSDs

Policies and practices surrounding CSD hardware and software use dictate how contractors, and often staff, manage which devices to use for projects and how to use those devices. Polices differ widely across the DOTs researched. The **Ohio Department of Transportation** (ODOT) conceives of anyone who isn’t staff to be in the same clearance category, whether they are contractors or universities. These

designations and their policies are more important than if the device is state- or contractor-owned.

ODOT next defines the level of the device based on whether or not it will touch the network, and if it does, what type of access the project requires. For devices that won't touch ODOT's production network, contractors can use their own equipment with ODOT software. In this scenario ODOT provides the hosted, offsite solutions to contractors to ensure ODOT's network security. Such hosted, offsite solutions utilize the network in a limited way and only have access to specific applications. In this way they are completely controlled.

That said, ODOT does not use many CSDs. They run pilot projects to determine the necessary hardware, then acquire it. 90 percent or more of all devices used belong to ODOT. It is much faster to configure their own devices to ensure security than to manage all of the variables with foreign devices. The 10 percent of foreign devices allowed by ODOT is determined by the applications that contractors need. In one project ODOT released a collection management software to count light poles at cloverleaf intersections. They launched their collector app in 30 to 45 days. When data collection occurs via a cloud based solution then it doesn't matter who owns the device; what matters is the security of the path to the application.

In the **Kansas Department of Transportation** (KDOT), CSDs are treated like any other piece of contractor supplied equipment, where the contractors have the latitude to purchase and dispose of devices as they like. KDOT's concern is with the devices that connect to their network, usually through a virtual private network[1] (VPN) port. To connect via a VPN port contractors must comply with State of Kansas security policies.

Massachusetts Department of Transportation (MassDOT) uses CSDs that are written into District contracts. MassDOT is organized into six districts, where each district operates autonomously, makes their own contracts, and tracks their own devices, independent of Central Operations, similar to Ohio.

Virginia Department of Transportation (VDOT) prohibits the use of CSDs on its network unless they are required to meet the contract's needs. For CSDs to be used on a project the scope of work (SOW), service agreement or contract must that. In order to maintain security on VDOT's network, CSDs must meet the same security controls as does VDOT equipment. All CSDs must have antivirus software and firewalls that are VDOT approved, software and updates must be current and contractors must pay to install and maintain these security measures.[2]

The **Georgia Department of Transportation** (GDOT) doesn't have one set policy surrounding CSDs, but allows the contracting agency to decide and set its own internal

[1] A VPN is a digital network within another physic computer network, which allow individuals access to protected information stored on a private network.

[2] Solicitation / Contract / Order for Commercial Items Offeror to Complete Blocks 12, 17, 23, 24, & 30; Standard Form 1449

policies and standards, so long as they don't conflict with existing laws, policies and standards. The contracting GDOT agency determines whether or not CSDs will be allowed based on a risk assessment that complies with State standards; if allowed, the CSDs must be accounted for in the agency's system security plans. The GDOT agency that conducts the risk assessment should consider: sensitive information; encryption, remote wiping, locking capabilities or tracking in the event of a lost or stolen device; wiping the device of data at the completion of a project; the legal considerations of enforcing all of these elements.

The **Alabama Department of Transportation** (ALDOT) manages contractor knowledge of devices differently: contractors must provide a separate technician-level session which includes "hands-on" instructions for using ALDOT's system, a laptop computer with the manufacturer's configuration and diagnostic software, system test equipment, and any other Contractor supplied equipment.

Similar to ALDOT, the **New York State Department of Transportation** (NYSDOT) requires that contractors provide their own training, at least regarding the Document Control System (DCS). The DCS training is organized, coordinated and provided by the contractor. The training consists of covering the needed accommodations, materials, personnel, services, travel and everything necessary to facilitate the training. However, if being provided to NYSDOT staff, the contractor is not responsible for travel and accommodations of those individuals.

Contractual Mechanisms and Procedures

Regarding the contractual mechanisms and procedures, it is instructive to begin with contractor liability. ODOT has had unsavory experiences with third party contractors on the software side. The transportation market is relatively small, as is the number of vendors that produce useful software, so not all software produced is good.

ODOT recently experienced an issue with vendor software that stopped work, which is very costly to the Department. In one example a fuel management system wasn't performing properly so ODOT sued them; the next vendor correctly deployed the fuel management software. If ODOT encounters other faulty software they give the vendor 30 days to rectify, and if it isn't rectified within that period then the Department will pursue adjudication. Due to several experiences with contractor culpability, which resulted in losses for the Department, ODOT has taken a more aggressive stand on contractor deliverables and time periods.

If a deliverable is unsatisfactory, it can be difficult to determine culpability, between the contractor and Department, or which group within the Department. For example, if ODOT is dissatisfied with data results due to technical problems then that is an IT issue, but if ODOT is dissatisfied with data gathered with functional equipment then it is a business problem. Because of that, it is rare for IT to see contracts that are related to business problems. If unsatisfactory data collection is a business issue then IT will help them decide whether to use contractors or employees, but that is a business, not a technology contract.

If stipulations aren't fulfilled and contractors don't utilize hardware of software correctly, don't collect data correctly, produce a software correctly, or generally satisfy the agreed-upon contract, it could have significant consequences for a DOT: stopping work, slowing work, or building workarounds. The best practices in holding contractors liable for hardware, software and related deliverables is to give them 30 days to correct the problem and if uncorrected after that time, to resolve it through adjudication.

Another important consideration for contractual mechanisms and procedures is device inventory. ODOT is divided into districts, where the districts manage their inventory, applications, locations, loaning and receiving of devices. Due to this there are 12 different processes for loaning and receiving devices. ODOT operates like a collection of fiefdoms, where the central headquarters makes suggestions, not mandates, to the districts. NJDOT does not follow the fiefdom structure; this structure works well in construction but poorly in IT because a lack of control over the districts lead to complications in data consistency.

The Headquarters-District dichotomy leads to a lack of control over inventory management; it also leads to data consistency problems. For example, 12 districts may collect the same information in 12 different ways; some districts input "street" another "St." and another "St". This creates tremendous inefficiencies across ODOT and requires additional time, resources and interventions to correct.

Districts can borrow equipment from each other and share assets. To exemplify District-Headquarters relations, last year ODOT Headquarters replaced all engineering computer aided drafting (CAD) machines with new versions. However, the result was that ODOT doubled the number of available machines because the Districts retained the old machines instead of disposing of them; ODOT Headquarters can only make recommendations to the Districts.

ODOT Headquarters used to issue mandatory quarterly and annual device tracking reports but no longer does this. ODOT also used to have software and hardware licensing details organized but also no longer does this. Each District is only responsible for the devices in their jurisdiction and there is no standardized quality control (QC) about asset location. Once a year each division does a touch inventory then reports back to their district headquarters. But this is District- , not Headquarters-driven.

Purchases and standards used to be operate on the district level but now ODOT does bulk purchases and sets the standards. In terms of standards, it is a matter of what ODOT is willing to support. Committees determine what hardware and software ODOT supports, then the districts must abide by these standards.

The maintenance and archival of data gathered with CSDs is just as important as any of the aforementioned steps. Indeed, it may be considered one of the most important, as many times this is considered the end product for a project. There are many crucial elements in the world of archiving data and CSDs, but one is how data and information stored on CSDs are transmitted to states during the project closeout process.

The **Maryland Department of Transportation** (MDOT) handles this through what they call “end of contract transition,” where any outstanding data deliverables are transferred to them at one time, but through whatever means makes sense depending on the file sizes: email attachments (small files) or the secure FTP site (large files).

The **North Carolina Department of Transportation** (NCDOT) handles project close-outs in a more “manual” fashion, but going through the deliverables and making sure the data requirements have been met – that they are checked in and ready.

CSD Data Management and Information Security

Data access and ownership is a big concern for many DOTs. While most DOTs do own the data when they pay contractors to collect it, unfettered data access is equally acceptable to data ownership. Data collection and transmission varies widely depending on the type of equipment that is being used and its relationship to the network; all of the following are possible: automatic collection and transmission, transmission via a VPN, transmission by directly tapping into the hardware. For most mobile equipment, the data is transitory to the device because it collects data then transmits it once it connects to the network. Once the data is collected and transmitted to a repository, it is cleansed and then automatically transmitted to a DOT database, or manually fetched from the repository. Backing up the data may occur automatically and DOTs may also use vendors for back up.

In order to continue improving these systems and their relevant hardware and software, DOTs sometimes run pilot projects for research purposes. One issue that DOTs have encountered is that pilot projects are so successful that customers want to keep using them as production-level platforms. To prevent this research projects must have defined time periods and end points after the criteria for success is met; it could also help to clearly outline that the pilot project is for research purposes and will have a finite utilization period.

Data Transfer

KDOT typically uploads data through a VPN, to a secure website, before it is scanned and downloaded into a KDOT system. KDOT occasionally shares project documentation through a SharePoint site. ODOT has a similar policy: all third party contractors use a VPN for network access and they sign high value data indemnification agreements (entire agreement, not just a clause.) to ensure the contractor cannot cause ODOT losses of any kind.

MDOT uses three methods to transfer data from devices to their servers: email attachments for frequent, small files; a secure file transfer protocol[3] (FTP) site for infrequent, large files; ProjectWise[4] software for frequent, large files. Regardless if the device is a CSD or state-owned device, email attachments are the most common form of data transfer and small files that are frequently submitted. MDOT only allows state-owned

[3] FTP is a standard network protocol used to transfer files between a device and a computer server

[4] Engineering project collaboration software produced by Bentley Systems

devices to access their VPN (this secure connection is mainly used for large file transfer, and files go directly into the desired database), so they created an FTP site for CSDs to transfer large files on an infrequent basis. The benefits of the FTP site are that large files don't slow down GDOT's network, and it is easy for contractors to access. For example, contractors will go to the MDOT website, enter through a username and password, and both upload and download files there; it can be structured so that if there are 10 different projects there are 10 different directories.

Finally, MDOT uses ProjectWise primarily for very large engineering files that must be transferred frequently and would be cumbersome for the FTP site. Regarding the frequency of data transmissions, data is transferred based on whatever is designated by the terms of the contract; sometimes this means annually, it could occur more often, and sometimes the data is only transferred at the end of the contract, during what is called "end of contract transition."

Similarly, **NCDOT** doesn't allow CSDs to connect to NCDOT's VPN because that is reserved for state-owned devices only. CSDs transfer data and documents through Microsoft SharePoint and SharePlus (the mobile app that connects to SharePoint), which are collaboration and document sharing applications. NCDOT uses a secure sockets layer[5] (SSL) to make sure that documents transferred in this way are secure.

Depending on the type of project and contract, NCDOT highway project data is primarily transferred continuously throughout the project. A typical highway project has 100 milestones, so data is transferred at the close of each milestone. Contractors can also send raw data through a synchronization application that will pull information from a device into a holding location where it gets scanned, before it can be fetched by a NCDOT employee. Unlike other DOTs, NCDOT strictly forbids data transfer via USB drives or CDs.

By contrast, the **Oregon Department of Transportation** (ORDOT[6]) receives data collected by CSDs on disks, thumb drives or portable hard drives; but more commonly files are transferred via FTP or a cloud-related service. ORDOT is currently in the process of implementing an engineering data management system that will allow external project partners access to ORDOT project files. Users of state-owned devices can transfer data through a VPN, which is the most common form of data transfer, or through the same methods of CSD users. Some state-owned devices can't connect to the VPN only in the event that ORDOT is time-constrained and needs the devices in the hands of the contractors as soon as possible.

NYSDOT calls its data / document transfer system the Document Control System (DCS) Any contractor hired by NYSDOT must provide their own IT support and equipment that is compatible with NYSDOT's Document Control System (DCS). This system is used to

[5] SSL is the standard security technology for establishing an encrypted link between a web server and a browser

[6] Oregon DOT refers to itself as ODOT, as does the Ohio DOT; because of this, and to prevent confusion throughout the document, Oregon DOT shall be referred to as ORDOT

send and receive documents between NYSDOT and its contractors; the NYSDOT point person which facilitates the DCS is the Document Control Specialist. The contractor's equipment must contain the necessary software to access the DCS, and both hardware and software must be configured such that the documents are in a format that is viewable by the department. NYSDOT provides these hardware and software requirements in their requests for proposals (RFPs).[7]

In order to facilitate functionality of the DCS and its interface between NYSDOT and contractors, the contractor must furnish NYSDOT with valid email addresses for all authorized contractors. To ensure the security of NYSDOT's network, contractors must have the appropriate anti-virus applications on their devices. Finally, similar to the aforementioned processes where the contractors are responsible for the hardware, software, internet and following NYSDOT protocols, contractors are responsible for their own technical support. It is important to note that all information that resides on the DCS server shall become the sole property of the Department.[8]

Data Access and Information Security

Almost all data that **ODOT** collects is transitory to the device: the device collects and then automatically transmits the data when it connects to the network. ODOT has a digital media center (DMC) host server where the data is stored. ODOT regularly pulls data from this server and backs it up. The process is that data is collected, scrubbed, delivered and automatically backed up. ODOT also uses vendors to back up data, while internal data is backed immediately after scrubbing.

Data scrubbing, or cleansing, is a network security measure that all state DOTs take. One example of ODOT security measures is the following: ODOT works with the University of Akron and the University of Bowling Green. In one project ODOT bought servers, Akron deployed them, then Akron wanted to connect them back into ODOT. But security protocol prohibits this; ODOT must work with an active directory and architecture standards. This type of server must be isolated from ODOT's network until it undergoes security clearance. Universities want unfettered access but that cannot happen; they must work on their own virtual local area network[9] (VLAN) until whatever server or data or processes are screened to meet ODOT standards.

While security measures are necessary, it can be a fine balance between security protocol and efficient productivity. For ODOT, more policies and practices leads to less security, while ODOT's focus is on mobility. ODOT is trying to automate many things with end user experiences in mind, use less paper and use any device to achieve their objective. For example, ODOT is trying to integrate contractors' horizon environment,

[7] Item 639.30030002 – Document Control Management

[8] Item 639.30030002 – Document Control Management

[9] A VLAN is a group of workstations, servers and network devices that appear to be on the same LAN despite their geographical distribution

license management tool and mobile device management tools to improve contractors' working experience while maintaining strict security measures.

ODOT does not own intelligent transportation systems (ITS) data, nor weather and speed sensor data; ODOT contracts these services out and does not own the data but has unlimited access to them. Speed data is constantly being collected, calculated, and transmitted every few minutes. The vendors transmit the data to a trusted host location, from where ODOT fetches it as it wishes, after confirmation that the data are clean. Because of that, data ownership is not a concern, but data access is; as long as ODOT can access the data it needs to then possession is irrelevant.

The **California Department of Transportation** (CalTrans) has robust security processes and protocols in place: Caltrans contracts contain very specific encryption standards, as well as reference to IT Security requirements contained in the State Administrative Manual. These requirements include:

- Encrypt all State-owned data stored on portable computing devices and portable electronic storage media using government-certified Advanced Encryption Standard (AES) cipher algorithm with a 256-bit or 128-bit encryption key to protect Caltrans data stored on every sector of a hard drive, including temp files, cached data, hibernation files, and even unused disk space.

- Encrypt all State-owned data transmitted from one computing device or storage medium to another

- Install and maintain current anti-virus software, security patches, and upgrades on all computing devices used during the course of the Agreement

If a state combines strict encryption and IT security standards with a broad definition of "state-owned data", that would make for a very effective information security policy. However, these types of clauses also have the following problem:

- Smaller firms or firms without robust IT resources or budgets may not be able to achieve compliance with these standards, which could limit the pool of available and qualified contractors.

Maintenance and Archiving Data from CSDs

Long-Term Maintenance of Government Records

Another important part of archival is the long-term maintenance of government records. **GDOT** manages this through a department called Records Management, which manages the archiving based on the agency, State or Federal data, and other regulatory requirements.

MDOT manages this by having different servers, files and databases for different kinds of data and records. That said, MDOT wants to move towards a deeper archival system for older project data, instead of having all data on the same network. Such a system

would increase the speed and ease of searches, as old projects would be part of the database if people forgot to mark them as “inactive,” and it would be cheaper to archive older data this way. MDOT manages data and document storage through a series of internal servers and directories: file servers, database servers, application servers, and sometimes other offices manage their own servers, all of which are locked down to State data security standards.

MDOT allows the contract holder to get a request for employees and contractors to access parts, or all, of a server. At this stage it is still considered right-based and is not open to the public; the public can access information through MDOT’s website or the Maryland state data portal, which publicizes non-sensitive information.

By contract, **NCDOT** doesn’t differentiate between Federal, State and local data and documents, but stores them all on the same large file server. NCDOT will store data this way for three years then move them to different servers. NCDOT grants public access through its website or the North Carolina Communications Office website, where the public can make an information request or Freedom of Information Act request.

GDOT makes decisions on public release of records based on data security and business need, on guidance from the Agency and their legal department, which determine the requirements.

Data Remaining on CSDs after Contract

After data and documents have been transferred to a DOT, they have been properly archived, and the project is closed out, there may be a concern that this data still lingers on the CSDs. How states manage this differs:

GDOT’s policy is that at the end of the project the business unit that contracted the project will ensure all the information has been wiped from the CSDs; agencies define their own security policies and standards and contracts to ensure that no state information is unsecured at anytime.

By contrast, **MDOT** has taken the stance that if devices are not state-owned then they don’t have the authority to bring them in and prove that they have been wiped. If a firm was contracted to deal with confidential or sensitive data, then MDOT puts language into the contract where the contractor must submit something in writing that states the data was wiped; this is in the event that MDOT needs to take legal recourse. MDOT has never seen a case where devices are brought in to prove they have been wiped; in such a case CSDs should have not been used. MDOT encrypts all confidential data that is archived on its servers, while non-sensitive data is not encrypted; on-site contractors can only access these servers through secure log-ins.

Similarly, **NCDOT** doesn’t take steps to ensure wiping of CSDs after project close-out; these devices were never connected to their network and they can’t access them. Furthermore, the final products belong to NCDOT (while any ancillary products belong to the contractor), which should prevent any data access concerns in the event of

liability or lawsuit. Unlike MDOT, NCDOT doesn't have any policy that requires contractors to wipe their devices.

ODOT contractors can access emails and texts from devices but these messages are encrypted. Texts have the potential to be public records, regardless of the ownership of the device, if they were made during working project hours. Currently there is no policy for texting, on or off devices, but if someone requests these files they are readily available to ODOT.

Responding to Open Public Records Act Requests and Pre-Trial Discovery

All of these issues regarding archiving and open public records revolve around data access: the ability to access data from a CSD retroactively, after project close-out, in the case of DOT liability or a lawsuit is important.

MDOT manages this through its understanding of data ownership: all data that MDOT paid for is transferred according to the contract, and at the project close-out; any data that MDOT didn't pay for they don't get nor have access to while the project is open or after it closes. If a contractor built a system to help themselves produce a deliverable or collect data, then this system would be retained by the contractor and not given to MDOT; MDOT is not sure why a contractor would collect data if they are not paid to do so.

For **GDOT**, State policy states that an agency shall make a provision in the engagement contract that at the end of contract all state data shall be handed over to the state agency. After that the agency determines the availability of its data.

ODOT also has a provision to access data; they recently added a specification[10] to their 2015 Standard Specifications for Construction and their construction contracts that requires contractors to provide ODOT access to all project-related information. The specification seems to focus on contract-related data, but could be construed to include engineering data.

For **Florida Department of Transportation (FDOT)**, the Florida Sunshine Act is one of the broadest and most demanding public records laws in the country. Basically, any and all project records (other than trade secrets as defined by the State) must be preserved and made available to the public upon request. FDOT takes a unique approach to this requirement in its contracts. Based on recent changes to the Florida Sunshine Act, FDOT has updated its standard contract to require the following:

- Contractor is required to maintain public records in accordance with the law
- Contractor has the option of providing FDOT with copies of the records in response to a public records request rather than the contractor making the records available itself

[10] Section 00170.01; Appendix G

- Contractor has the option of keeping the public records after completion of contract rather than turning over all records to FDOT; however, if Contractor elects to retain the public records, Contractor must then respond to public records requests it receives from FDOT

- If contractor fails to comply with the public records law, FDOT's remedies can include immediate cancellation of contract and application of penalties consisting of the cost of FDOT's enforcement of the law including attorney's fees

FDOT also uses a broad ownership clause to obtain ownership and control over all project data ("All tracings, plans, specifications, maps, computer files and/or reports prepared or obtained under this Agreement, as well as all data collected, together with summaries and charts derived therefrom, will be considered works made for hire and will become the property of the Department upon completion or termination without restriction or limitation on their use and will be made available, upon request, to the Department at any time during the performance of such services and/or upon completion or termination of this Agreement"). This clause is effective for the following reasons in particular:

- Refers not only to "work product" or "deliverables", but also to "data", "computer files", etc.

- Is not limited to files and data first produced or created under the agreement – it also applies to data and files prepared, obtained, or collected under the agreement. This could apply to data and files that pre-existed the agreement, but which were obtained or collected from third parties or the state itself

- Requires the Contractor to make the data and files available to FDOT upon request at any time, both during and after the agreement

However, this type of clause has its drawbacks as well:

- Does not offer effective protection to contractors who may be obtaining proprietary data from third parties or who may be using their own proprietary intellectual property for performance of the services

- Does not specify how the data should be provided to the State

Task 2 – Develop and Field Test Survey

Following the research review, the research team drafted a survey instrument to gather information on the deployment and use of CSDs, how information stored on CSDs is managed, and how information is transmitted between CSDs and NJDOT information systems and file servers.

The survey released to NJDOT employees included the following questions, covering employee background, CSD use, tech support, information collection, management & sharing and lastly, email usage on the devices:

Background Questions

1) Please identify the Division / Bureau with which you work:

2) What is your Civil Service title?

3) What is your functional title?

4) Have you ever worked as a Resident Engineer?

5) Where do you work?

6) Do you expect to use a contractor supplied device (CSD) in the near future (NOTE: a CSD is defined as an electronic device provided to NJDOT staff by a vendor, supplier, consultant, subcontractor, or contractor, including a university)?

7) What type of individually assigned device(s) do you use for NJDOT work?

CSD Use Questions

8) Based on your experience, what is the greatest number of shared CSDs that have been assigned to all NJDOT staff in a single project?

9) What is the total number of NJDOT projects you have worked on in which you were issued a CSD?*

10) What percent of the NJDOT projects you have worked on have you used CSDs?*

11) Do you prefer using CSDs over NJDOT electronic devices?

12) Why do you prefer CSDs over NJDOT electronic devices?

13) How often do you use your devices to do NJDOT work in a given day?

14) Which of the following security protections were installed on the CSDs that you have used?

Tech Support Questions

15) Have you ever sought technical support for CSD/NJDOT devices?

16) How often do you seek technical support for your electronic devices in a given month?

17) Who provides technical support for your CSD?

18) Have you ever needed technical support for your CSD during regular working hours?

19) Have you ever needed technical support for your devices during non-regular working hours?

20) How often do you seek technical support for your CSD and/ or NJDOT Supplied Device during non-regular working hours in a given month?

Information Collection, Management and Sharing Questions

21) Which of the following is used to transfer data from a CSD to another location or device?

22) Where do you store your data related to the NJDOT project you are currently working on?

23) Who is responsible for transferring the data from the CSD to another location or device?

24) How often is information transferred or uploaded from the CSD?

25) If you transfer or upload information from a CSD to a NJDOT computer, server, or cloud-based system, how do you do it?

26) If you do not upload electronically stored information, which of the following apply?

27) Do you believe uploading information from a CSD to a secure storage location is required by NJDOT or Division policy?

28) Do you believe uploading information from a CSD to a secure storage location is required by vendor contract agreements?

Email Use Questions

29) Do you access any email accounts on a CSD?

30) Which email do you access on a CSD?

31) How do you access your NJDOT email on a CSD?

32) Which email do you access on an NJDOT device?

33) Does anyone else have access to and/ or use one or more of the following email accounts on your individually assigned CSD?

34) Of the following, who has access to your CSD supplied email account from your CSD?

Task 3 – Deploy and Analyze Survey

The project team deployed the survey on the Survey Gizmo online survey platform. Upon conclusion of the surveying process, the project team proceeded to analyze the results of the survey on a holistic and question-by-question basis.

Survey Findings

A total of 394 NJDOT personnel participated in the web-based survey, although on a question-by-question basis, the number of respondents varied significantly. Based on the results of the survey the following findings became evident:

- Desktop computers and laptops comprise the majority of CSDs in use at the NJDOT, followed by cell phones, smart phones and USB drives. These proportions are relatively in line with the proportions of devices actually supplied by NJDOT. The exception to this trend is the issuance of smartphones. In the case of smartphones, a greater proportion tend to be supplied by independent contractors, rather than the NJDOT.

- Generally, employees utilize and interact with CSDs in the same way that they do with NJDOT-supplied devices.

- The majority of employees have not sought technical support for the use of devices, issued by the NJDOT or an independent contractor. Exceptions to this include desktops and laptops, issued by both the NJDOT and independent contractors. Additional exceptions are printers, fax machines, photocopiers and scanners. In the cases of these devices, technical support is sought primarily from independent contractors.

- NJDOT employees do not appear to have a preference for whether the NJDOT or an independent contractor supplies their devices. Rather, their preferences for devices are based on technological capabilities.

- The number one reason that NJDOT employees indicated that they preferred CSDs over those devices supplied by the NJDOT, is that certain devices are not actually supplied by the NJDOT. If NJDOT actually supplied these devices, employees would not have any issues using them as opposed to CSDs.

The survey results indicate that employees do not appear to have a preference for whether NJDOT or an independent contractor supplies their technological devices, so long as they run properly and contain necessary software. To follow, these results are further disseminated on a question-by-question basis.

Survey Results

Background Question Results

Question 1 asked respondents to identify with which division or bureau of the NJDOT they work. Almost half of all respondents work within the Capital Program Management Division, while approximately a quarter work within the Operations Division. The remaining respondents work within a range of other departments including Capital Investment Planning and Grant Administration (9 percent) and Transportation Systems Management (8 percent).

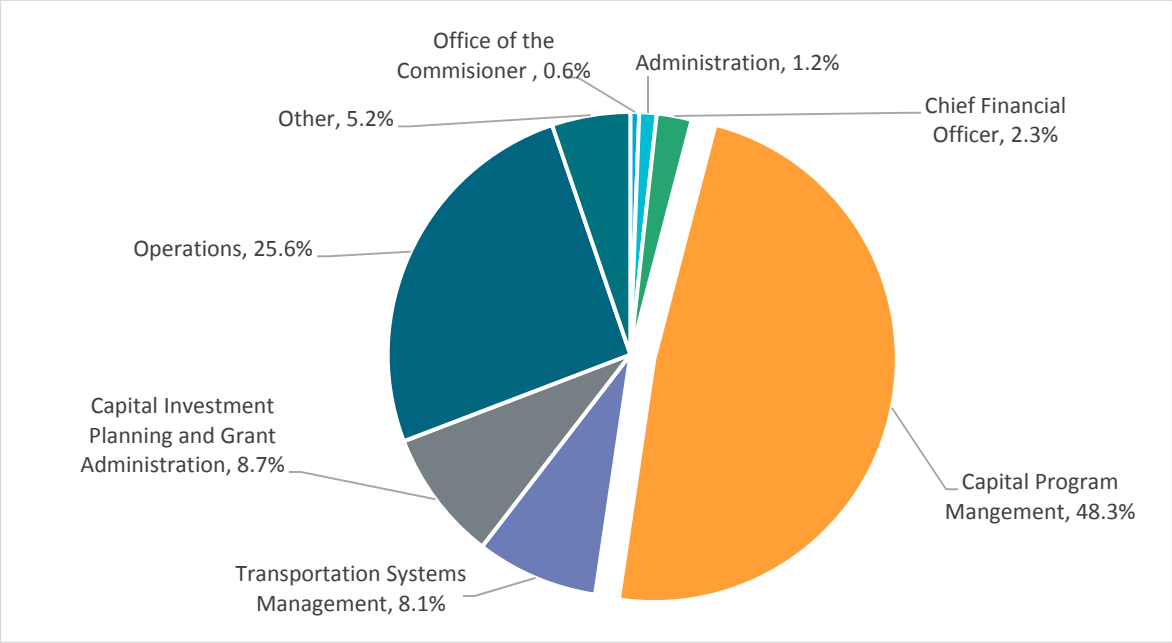

Figure 1. Question 1: Please identify the Division / Bureau with which you work

Building off of Question 1, Question 2 asked respondents to provide their Civil Service title. Given a total of 347 total responses, a wide variety of responses were provided. The most common response was 'Assistant Engineer' with 18 responses, followed by 'Principal Engineer' and 'Project Engineer' with 15 responses each. It should be noted that Question 2 was in the form of an open ended question. As a result, certain positions with the same title may have appeared multiple times. For example, in addition to 'Assistant Engineer', some respondents indicated their title was 'assistant engineer' or 'ASSTT ENGINEER', all of which would be considered 'Assistant Engineers'. It should be noted however that the majority of respondents to Question 2 hold an engineering or technical position. Question 3 asked a similar question, except referring to functional as opposed to Civil Service titles. 'Resident Engineer' received the highest number of responses at 29.

Question 4 asked respondents specifically about whether they have ever worked as Resident Engineers. About 14 percent of respondents (46 participants) indicated that they currently work as Resident Engineers. An additional 10 percent of respondents (34 participants) indicated that they had worked as Resident Engineers at one point, but do not currently. The majority of respondents, about 75 percent, have never worked as Resident Engineers.

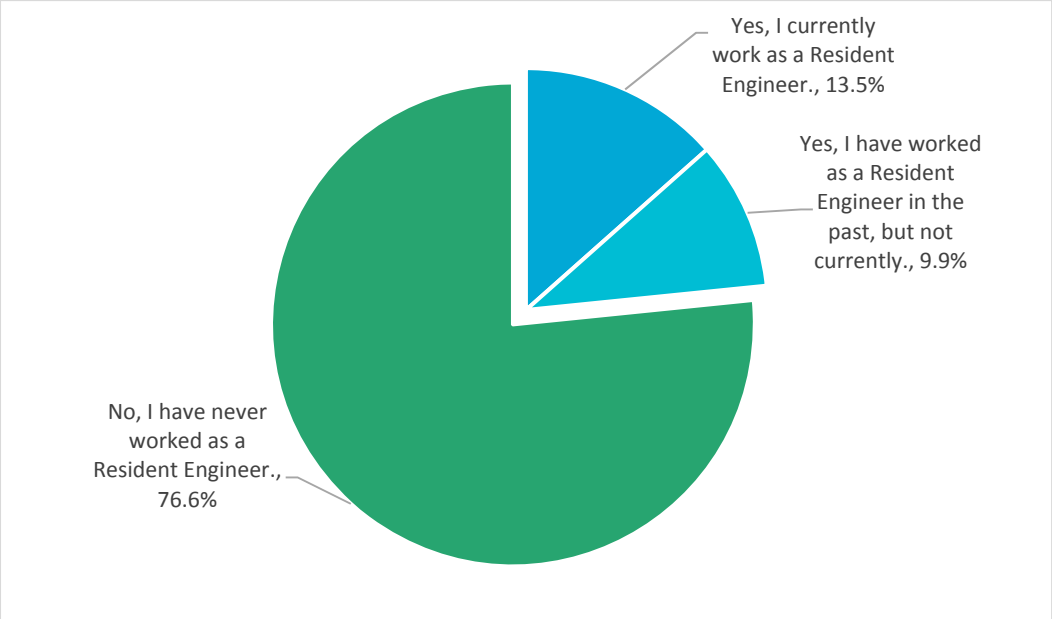

Figure 2. Question 4: Have you ever worked as a Resident Engineer?

Question 5 asked respondents where they work geographically. Just over half of the respondents indicated that they work at NJDOT Headquarters in Ewing. The remaining responses were split throughout the state with just under 10 percent indicating a regional office in Mount Arlington and Cherry Hill, or a NJDOT yard. Of those respondents that indicated 'Other', almost half identified some sort of field office or site.

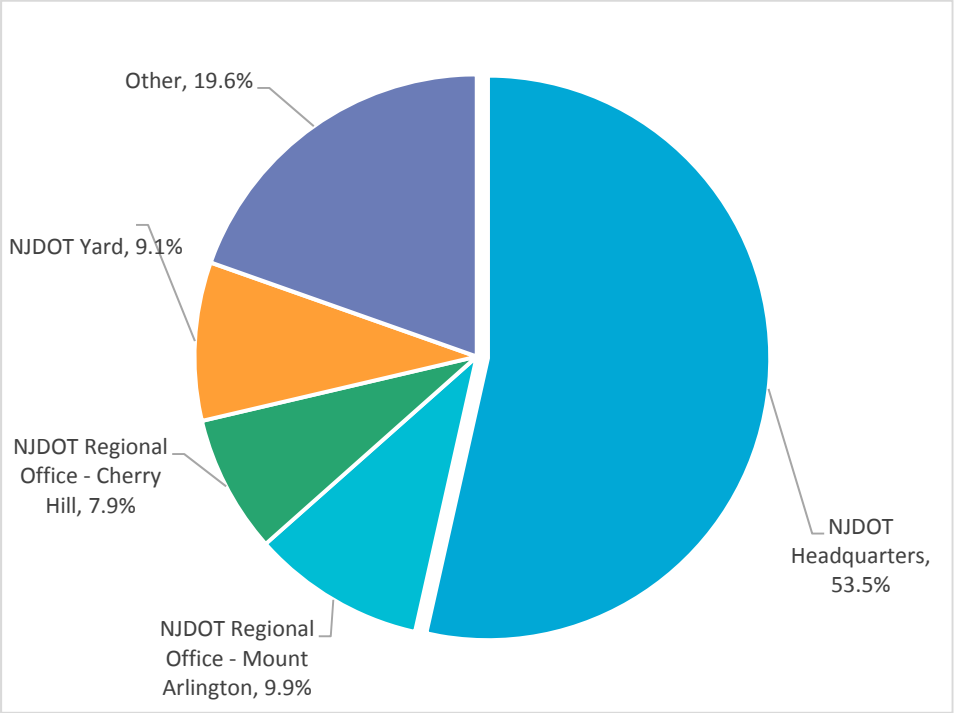

Figure 3. Question 5: Where do you work?

Question 6 asked respondents whether they expect to use a CSD in the near future. Almost two-thirds of respondents (214 of the total) indicated that they do not plan to. Of the remaining respondents, 37 percent of the total, most expect to use a CSD within 6 months. About 7 percent of all respondents expect to use a CSD within 12 months.

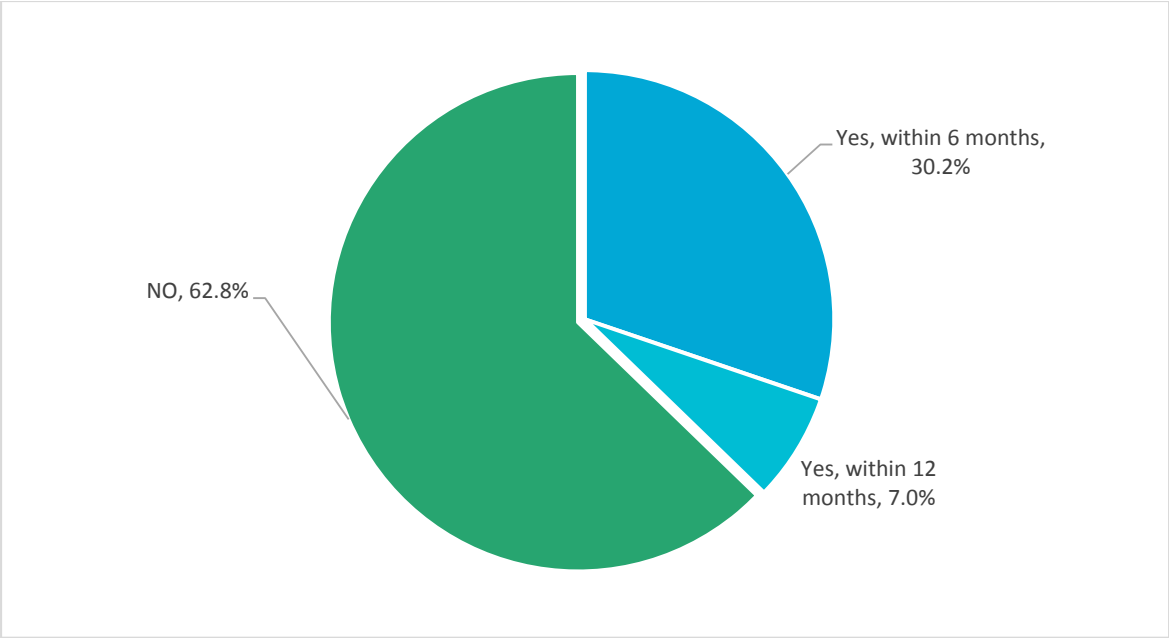

Figure 4. Question 6: Do you expect to use a CSD in the near future?

Questions 7 and 8 asked respondents which types of individually assigned devices they use for NJDOT work. Respondents were allowed to choose more than one device as needed. In addition, respondents were asked to indicate whether the devices were supplied by NJDOT, a contractor, or personal items. The most common indicated devices were computers (desktops followed by laptops). Additional devices frequently identified included USB drives, cellular phones and smartphones. The majority of such devices were supplied by the NJDOT, with a lesser extent of devices being supplied by contractors. It should be noted that most smartphones however were identified as personal devices. Question 8 asked those respondents who indicated 'Other' to list their device. Multiple devices, based on 18 responses were indicated, including cameras, scanners, an air card and a scanner.

Table 1 – Question 7: Which type of individually assigned devices do you use for NJDOT work?

	Desktop Computer	Laptop Computer	Tablet / iPad	External hard drive	USB drive	Cell phone	Smart phone	Other	None
Supplied by NJDOT	197	84	9	3	48	51	29	10	23
Contractor Supplied Device	71	46	17	20	43	34	50	7	61
Personal Device	16	25	20	14	24	46	65	3	43

CSD Use Question Results

Question 9 asked respondents, based on their experience, what is the greatest number of shared CSDs that have been assigned to all NJDOT staff in a single project. Proportionally, the results appeared to mirror the results of Question 7, with computers, either desktop or laptop, appearing to account for the most responses. Additionally, USD drives, cellular and smartphones also comprised high totals.

Table 2 – Question 9: What is the greatest number of shared CSDs that have been assigned to all NJDOT staff in a single project?

	Desktop Computer	Laptop Computer	Tablet / iPad	External hard drive	USB drive	Cell phone	Smart phone	Other
Number of CSDs	75	59	32	29	41	50	48	10

Question 10 asked respondents how many NJDOT projects they have worked on in which they were issued a CSD. Just under half of all respondents indicated between 1 and 5 projects, with an additional quarter of respondents indicating a number between 6 and 10 projects. Although the majority have worked on relatively few projects in which they were assigned a CSD, a few respondents did indicate larger numbers, with 5 respondents indicating over 25 responses. It should be noted that those respondents gave totals of between 50 and 100.

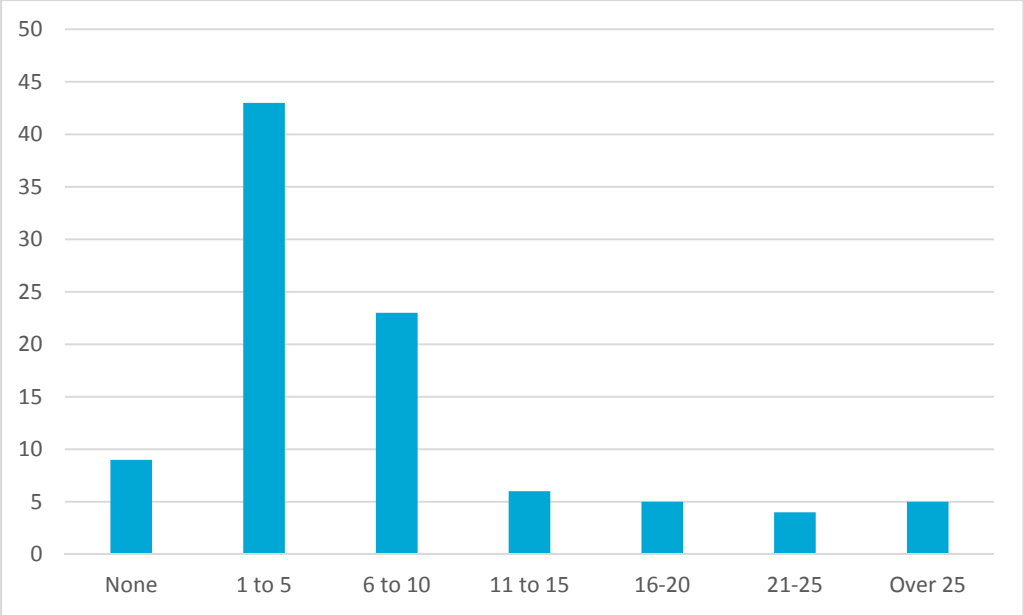

Figure 5. Question 10: What is the total number of NJDOT projects you have worked on in which you were issued a CSD?

Similar to Question 10, Question 11 asked respondents what proportion of NJDOT projects they've worked on in which they've used a CSD. Despite most respondents recording a small number of instances in Question 10, most respondents indicated that they've used a CSD greater than 75 percent of the time. This may indicate that most survey respondents have not been with the NJDOT for too long, or have been assigned to a smaller number of projects that are more time intensive.

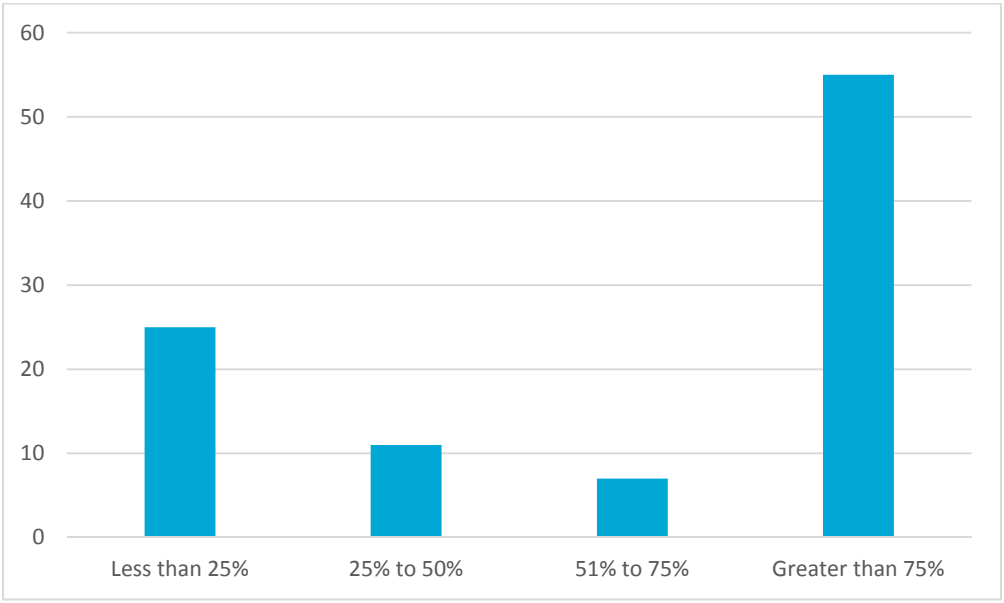

Figure 6. Question 11: What percent of NJDOT projects you have worked on have you used CSDs?

Question 12 asked respondents whether they prefer using CSDs over NJDOT electronic devices. Approximately two-thirds of respondents indicated ‘yes’. When asked why or why not, some respondents indicated better performing and/or newer equipment. However, multiple respondents indicated that they have no preference.

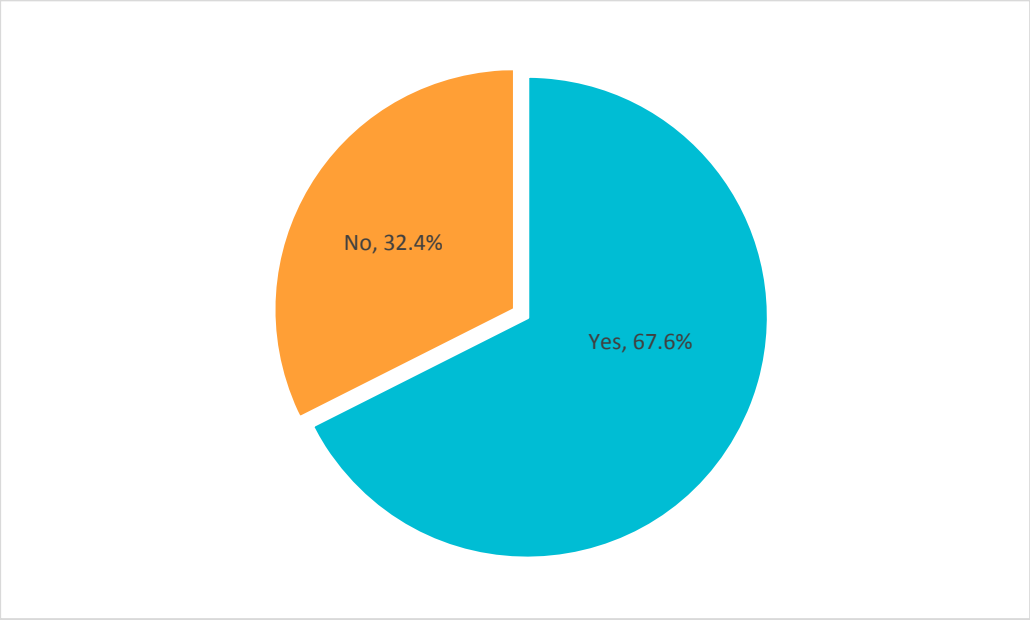

Figure 7. Question 12: Do you prefer using CSDs over NJDOT electronic devices?

Question 13 builds off of Question 12 by asking respondents why they prefer CSDs over NJDOT electronic devices. Results of Question 13 show that there was no decisive reason why respondents prefer CSDs. Of those responses however, the fact that there wasn’t a NJDOT device offered, was the most popular with approximately 25 percent of the total. The second most popular result was the benefits of technical support provided along with CSDs. This response received just under 20 percent of the vote. Other popular reasons included device speeds and the fact that NJDOT devices lacked specific functions needed to conduct work.

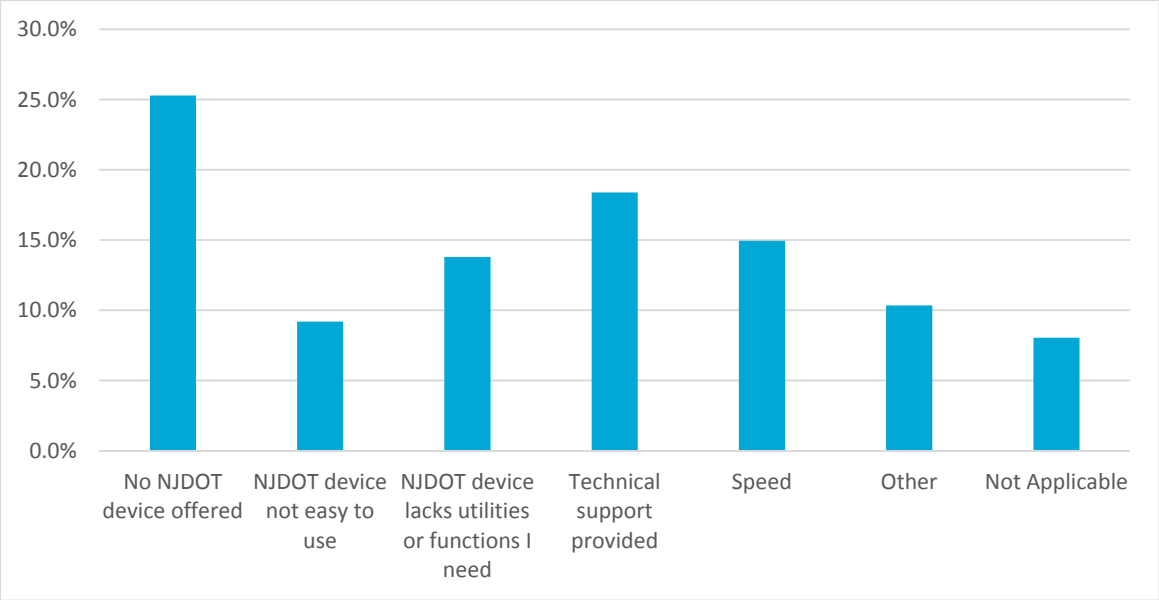

Figure 8. Question 13: Why do you prefer CSDs over NJDOT electronic devices?

Whereas the previous questions asked about the kinds of CSDs utilized and the associated reasons for using them, Question 14 asked about the frequency with which respondents utilize CSDs for NJDOT work. Respondents were additionally asked whether these were shared CSDs, individually assigned CSDs, or general NJDOT or personal devices. Results of Question 14 show that most respondents use their devices constantly or several times a day. This held true for CSDs, NJDOT devices and personal devices, with very few respondents indicating that they utilize their devices once per day or less.

Table 3 – Question 14: How often do you use your devices to do NJDOT work in a given day?

	Constantly throughout the day	Several times per day	Once per day	Once per week	Less than once per week	Not applicable
Shared CSD	29	20	5	3	3	34
Individually assigned CSD	48	19	5	0	3	19
Shared NJDOT device	9	7	2	1	4	59
Individually assigned NJDOT device	24	6	3	2	2	48
Personal device	11	17	0	4	9	43

With regards to security, Question 15 asked respondents which protections were installed on their CSDs. Respondents were allowed to select more than one option as

needed. About 75% of respondents indicated that anti-virus software was installed on their CSD, while just over half indicated anti-malware and firewall protections were in place. It should also be noted however that almost 25 percent of respondents were unsure of which, if any security protections were installed in their CSDs, while only 2 percent of respondents indicated that no form of security protections were installed on their CSD.

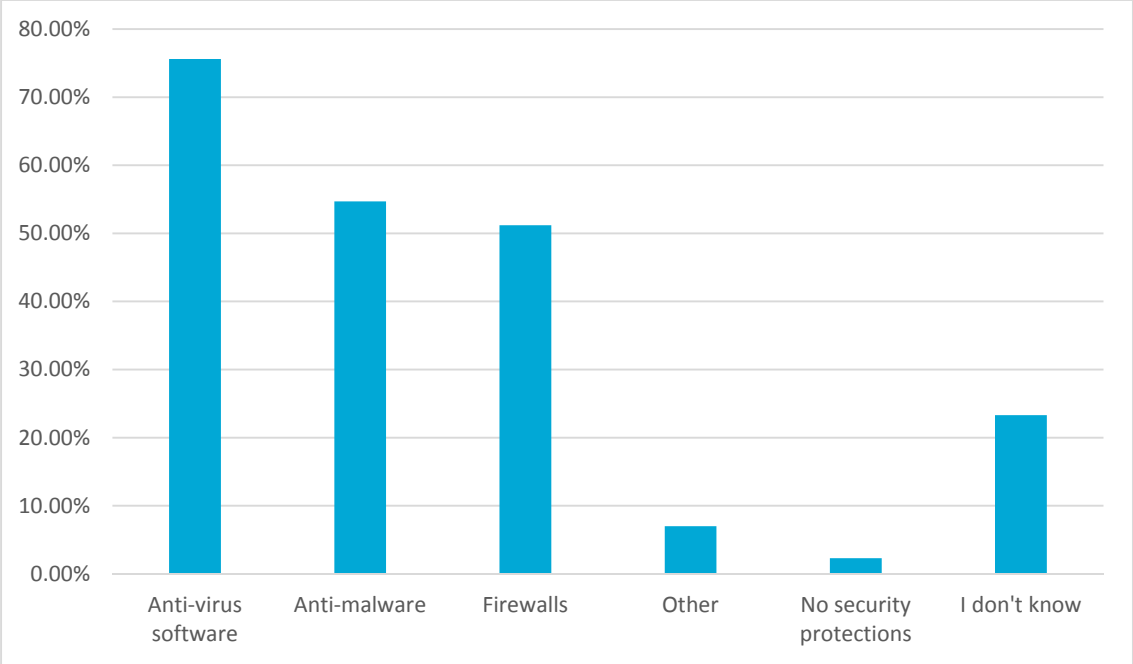

Figure 9. Question 15: Which of the following security protections were installed on the CSDs that you have used?

Tech Support Question Results

Questions 16 and 17 related to respondents receiving technical support for CSD and NJDOT devices. Results were broken out by device. Most technical support was sought for computers, issued by NJDOT, as well as in the form of a CSD. Additionally, respondents appeared to seek technical support more often for CSD printers, fax machines, photocopiers and scanners, than NJDOT-supplied devices. With the exception of these devices previously indicated however, most respondents have not sought technical support. For those respondents that indicated 'Other', Question 17 asked respondents to elaborate. Of these 13 respondents however, only 4 answered. Three respondents indicated 'None' while 1 respondent indicated that the contractor supplies technical support.

Table 4 – Question 16: Have you ever sought technical support for CSD/NJDOT devices? If yes, select all that apply.

	NJDOT	CSD	None
Desktop Computer	30	32	15

Laptop Computer	16	27	24
Tablet/iPad	4	8	32
External hard drives	1	4	35
USB drives	1	4	37
Cellular phone	5	13	31
Smartphone (iPhone, Android, Blackberry, Windows Phone)	5	12	27
Printers	18	36	11
Fax Machine	5	22	21
Photocopier	7	30	15
Scanner	9	27	20
Other	0	0	13
Not applicable	0	2	17

Additional related to the previous two question, Question 18 asked respondents how often they seek technical support. Most respondents indicated either 'None' or 'Less than once per month'. It should be noted however that although relatively infrequently, respondents sought technical support more for CSDs than NJDOT supplied devices. This was indicated by the fact that about twice as many respondents stated that they never seek technical for support for NJDOT supplied devices, while almost twice many respondents stated that they receive technical assistant less than once per month for CSDs compared to NJDOT supplied devices.

Table 5 – Question 18: How often have you sought technical support for CSD/NJDOT devices? Select all that apply.

	None	Less than once per month	1 time per month	2-5 times per month	5-10 times per month	10+ times per month
CSDs	20	48	6	5	0	1
NJDOT supplied devices	38	29	4	5	1	2

Questions 19 and 20 asked respondents about who provides technical support for their CSD. According to the results, over half of respondents stated that the contractor itself provided technical support. Outside vendors provided support to just over 10% of respondents, while the NJDOT itself provided support to a similar proportion.

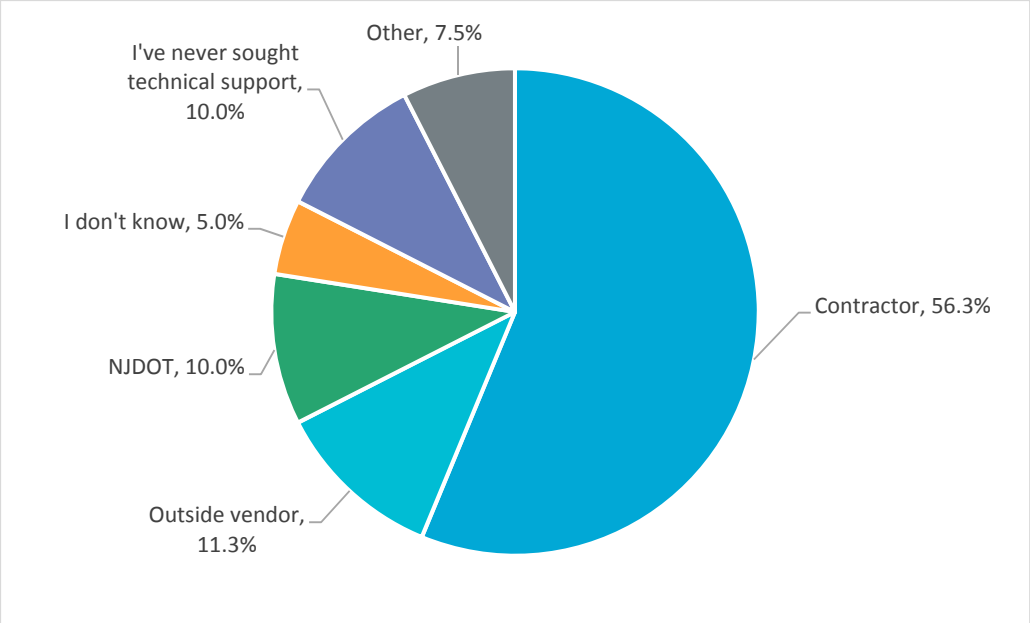

Figure 10. Question 19: Who provides technical support for your CSD?

Questions 21 and 22 asked respondents about when they've needed technical support for their devices. Question 21 asked respondents if they've needed technical support for their CSD during regular working hours. Of a total of 81 respondents, just under 75 percent (59 of the 81 total) indicated that they have, while 27 percent (22 of the 81 total) indicated that they haven't. Question 22 asked the same question, except with regards to non-regular working hours, while also breaking out the question into CSD and NJDOT supplied devices. Similar proportions were evident for both, though it should be noted that the question was not applicable for the majority of NJDOT supplied devices.

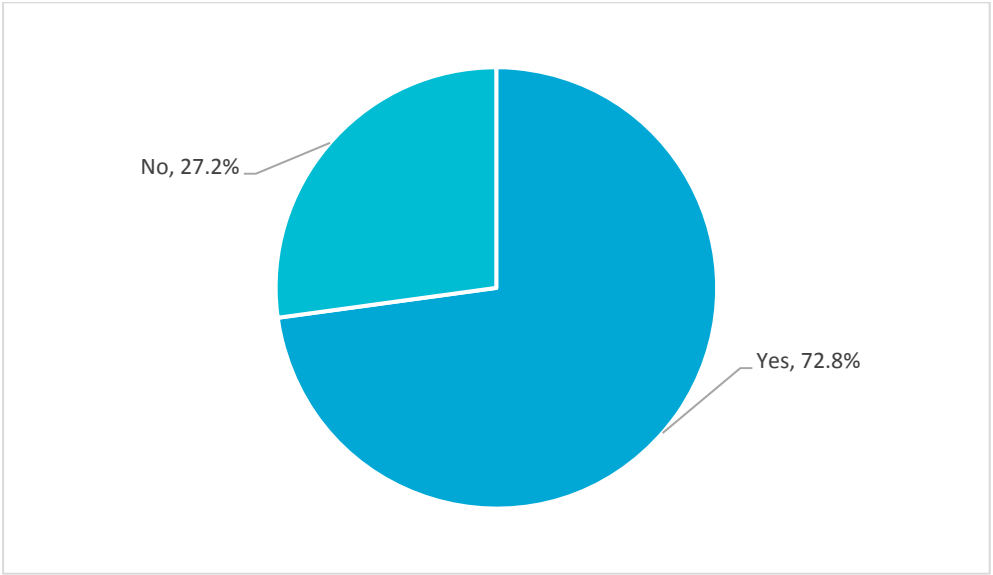

Figure 11. Question 21: Have you needed technical support for your Contractor Supplied Device during regular working hours (Monday through Friday 9:00 a.m. - 5:00 p.m.)?

Table 6 - Question 22: Have you needed technical support for your devices during non-regular working hours (Monday through Friday 5:00 p.m. - 9:00 a.m. and / or weekends)?

	Yes	No	Not applicable
CSD	15	55	9
NJDOT supplied device	11	33	35

Question 22 expands on Question 21 to ask how often respondents have sought technical support for their CSD and/or NJDOT supplied device during non-regular working hours. The majority of respondents, about two-thirds, have never sought help during non-regular working hours, while approximately one-third of respondents indicated that they have sought help less than once per month. Very few if any respondents indicated that they've sought help once or more times per month during the non-regular working hours.

Table 7 - Question 23: How often do you seek technical support for your CSD and / or NJDOT Supplied Device during non-regular working hours (Monday through Friday 5:00 p.m. - 9:00 a.m. and / or weekends) in a given month?

	None	Less than once per month	1 time per month	2-5 times per month	5-10 times per month	10+ times per month
CSD	54	24	0	1	0	0
NJDOT supplied device	57	18	1	1	0	2

Information Collection Management and Sharing Question Results

Question 24 asked respondents to identify how data is transferred from a CSD to another location or device. Out of 64 respondents, about 40 percent indicated that they manually transfer the data on their own. However, the next most popular response was that respondents were unsure of how this is done, representing 17 percent of all responses. With a similar total, 16 percent of respondents indicated that their data is never transferred. It should also be noted that cloud use and/or server synchronization accounted for just 11 percent of all responses, about a quarter of the amount that manually transfer by means of email, USB drive etc.

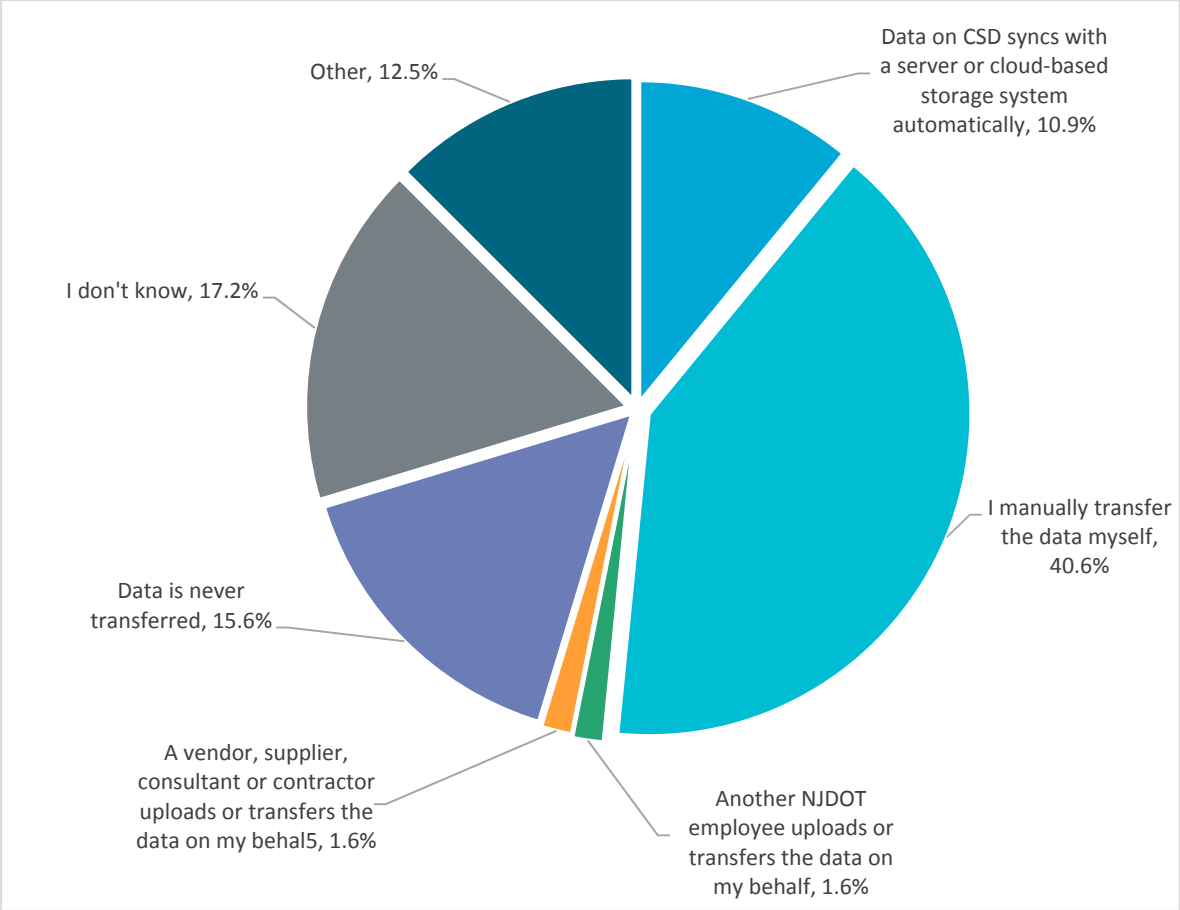

Figure 12. Question 24: Which of the following is used to transfer data from a CSD to another location or device?

Following the theme of device data, Question 25 asked respondents where they store data related to the NJDOT project they're working on. Respondents were allowed to select more than one option as needed. A computer, server, or cloud-based system maintained by a vendor, supplier, consultant, or contractor was used to store data by 70 percent of the respondents. Additionally, about 57 percent of respondents utilized similar methods maintained by the NJDOT. The remaining methods were utilized by well under 50 percent of the respondents, with the third most popular method being another contractor supplied device not already mentioned. Just under 30 percent indicated this method. It should be noted however, that a particularly small number of respondents answered Question 25, making the results potentially less insightful. A total of only 13 responses were recorded.

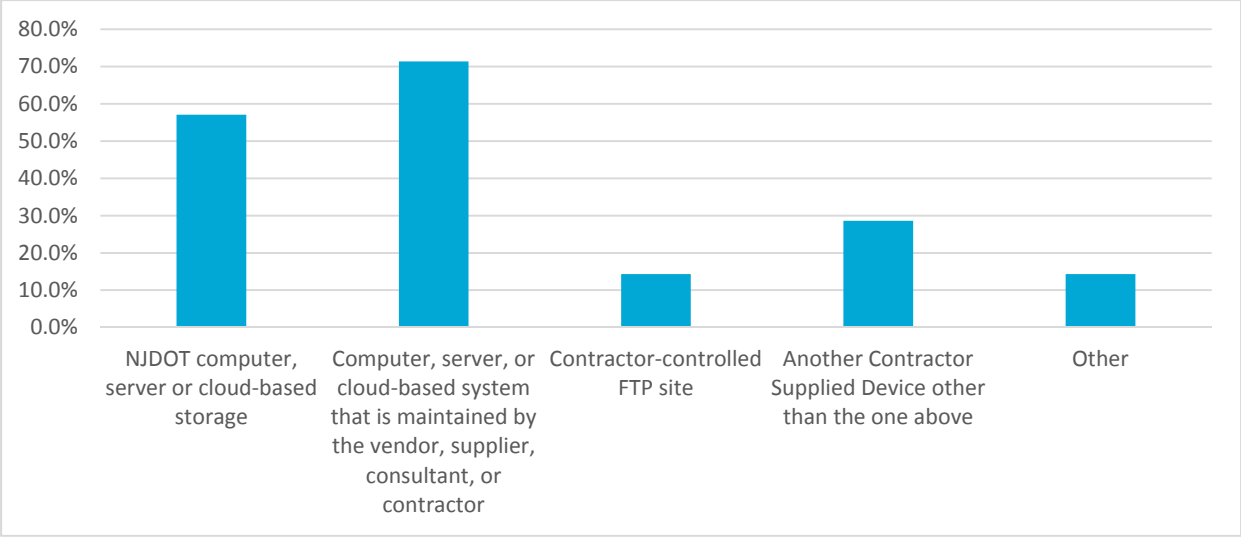

Figure 13. Question 25: Where do you store your data related to the NJDOT project you are currently working on?

Question 26 builds off of Question 24 by asking respondents who is responsible for transferring the data from the CSD to another location or device. Overall, both Question 24 and 26 are worded in a similar manner. Similar to the case with Question 24, most respondents (53 percent in this case) indicated that they manually transfer data on their own. The second most popular choice (20 percent of respondents) related to a vendor, supplier, or consultant being responsible for transferring the data. Together, these 2 options accounted for 75 percent of all respondent's answers.

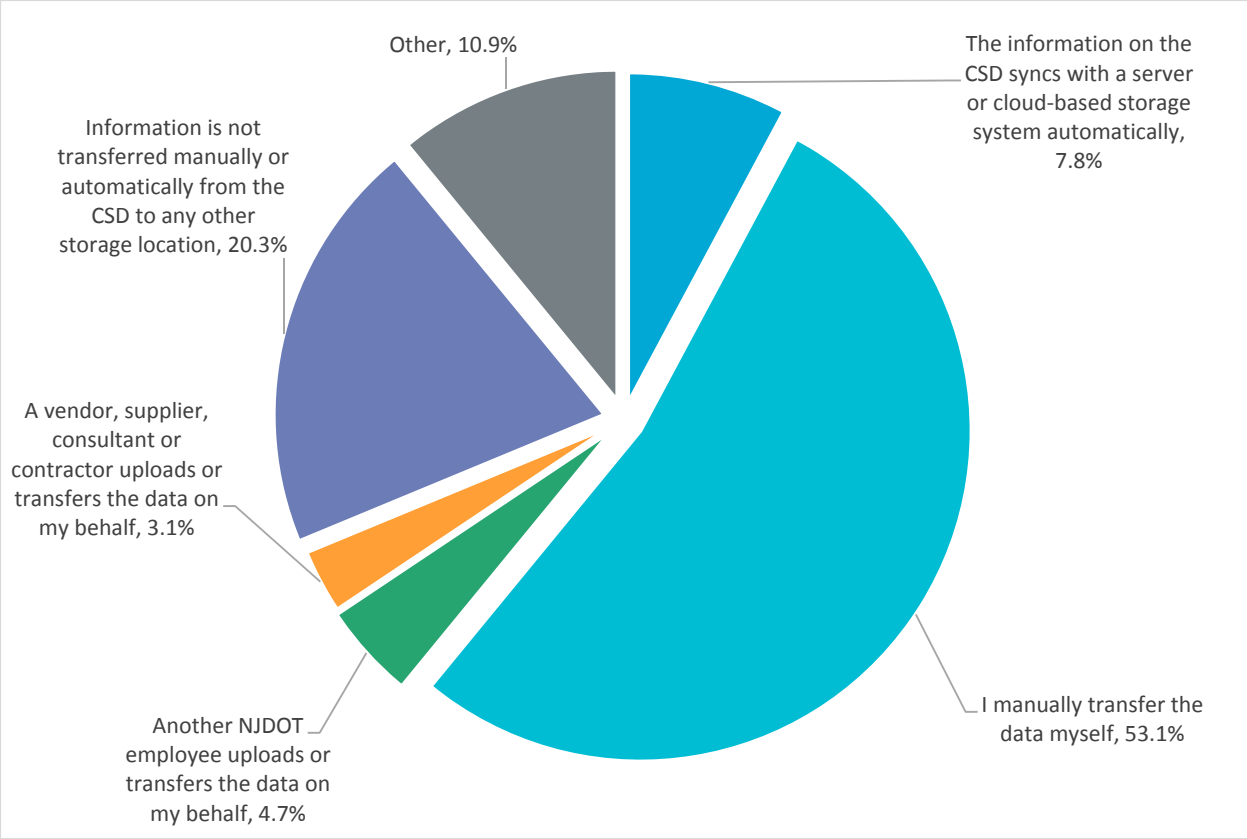

Figure 14. Question 26: Who is responsible for transferring data from the CSD to another location or device?

Question 27 asked respondents how often information is transferred or uploaded from a CSD. Respondents were asked to answer based on their answer to Question 24. For all methods of transferring and uploading data, respondents primarily indicated that they were unsure. This response comprised approximately 75 percent of the results. Of those respondents that did know, most indicated only as needed during the project. To a lesser extent, some respondents indicated either daily or also added 'at the end of the project' to 'as needed during the project'.

Table 8 – Question 27: How often is information transferred or uploaded from the CSD?

	Daily	Weekly	Monthly	Only as needed during the project	Only at the end of each project	As needed during the project and at the end of the project	I don't know

The information on the CSD syncs with a server or cloud-based storage system automatically.	6	0	0	8	1	5	42
I manually transfer the data myself.	7	4	3	12	7	6	22
Another NJDOT employee uploads or transfers the data on my behalf.	0	1	1	13	2	4	40
A vendor, supplier, consultant or contractor uploads or transfers the data on my behalf.	0	0	1	6	0	4	50
Information is not transferred manually or automatically from the CSD to any other storage location.	2	0	1	5	2	3	48

For those respondents that transfer or upload information from a CSD to a NJDOT computer, server, or cloud-based system, Question 28 asked respondents what method they utilized. Respondents were allowed to select multiple options as needed. The results showed that 3 methods were utilized by between 25 percent and 35 percent of respondents. These included the use of a USB/thumb drive and email. However, just over 50 percent of respondents indicated that they do not upload or transfer information from a CSD to a NJDOT computer server or cloud based storage system.

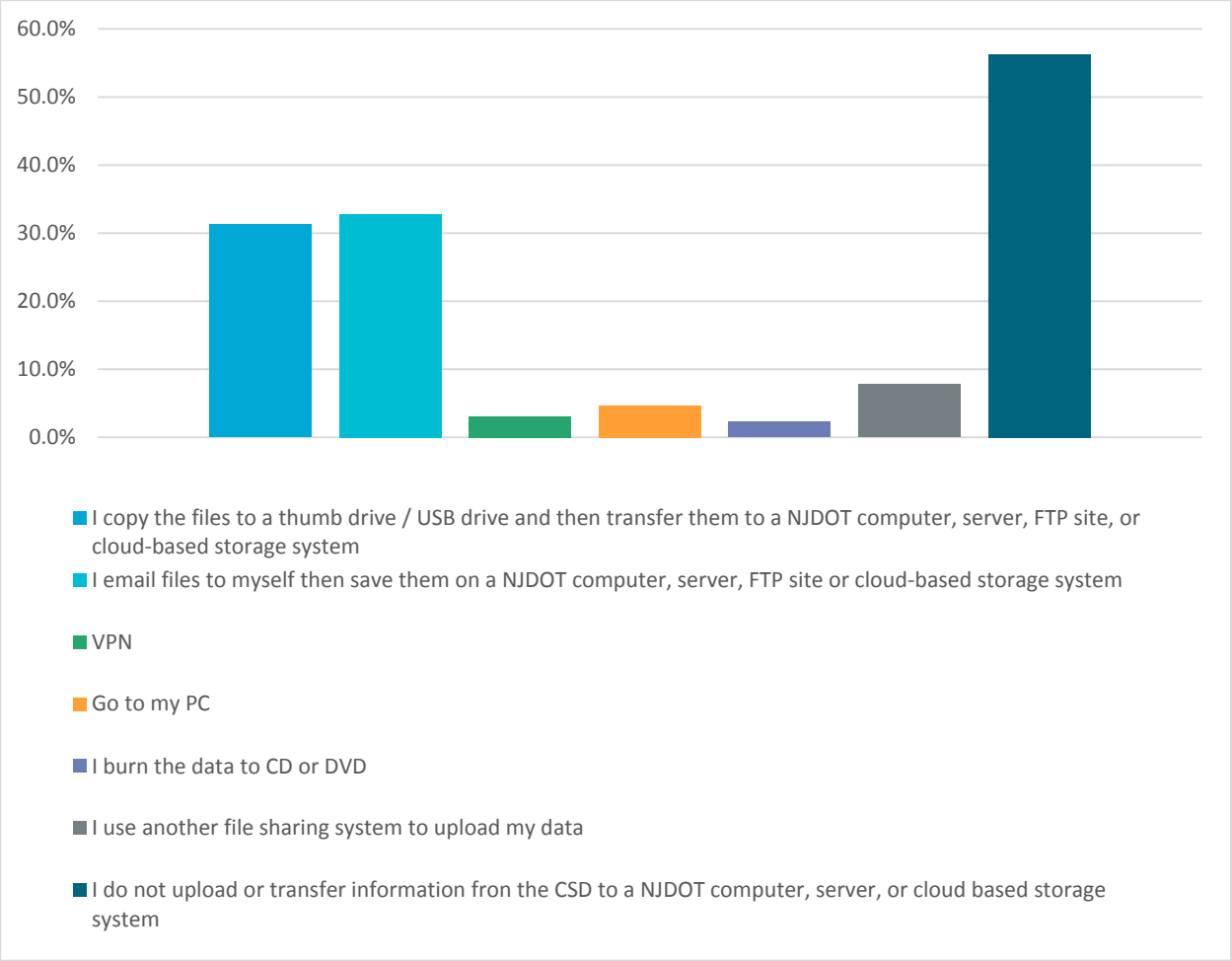

Figure 15. Question 28: If you transfer or upload information from a CSD to a NJDOT computer, server, or cloud-based system how do you do it (select all that apply)?

For cases where respondents did not upload electronically stored information, Question 29 asked for the reasons. Respondents were allowed to select multiple options as needed. The most common response, at just over 25 percent of respondents, was that all information on the CSD is deleted at the end of each project. The second most common response was 'Other' at just under 25 percent of respondents. A variety of responses were provided to elaborate on this response. Such responses included storage in a USB drive and the fact that hard drives are either deleted, removed, or placed in storage by NJDOT. Interestingly enough, 15 percent of respondents indicated that they print out hard copies and place them in a paper-based file.

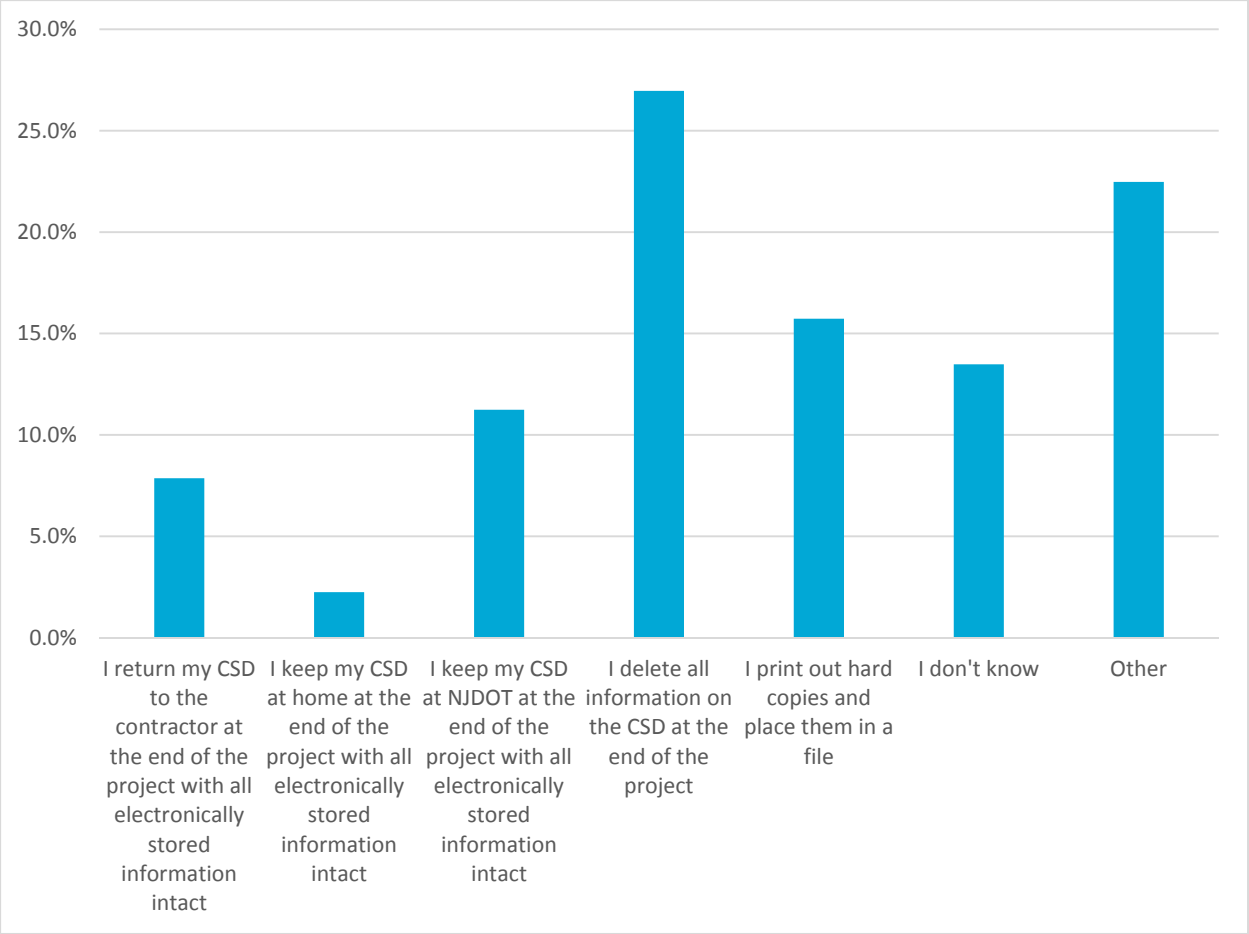

Figure 16. Question 29: If you do not upload electronically stored information, which of the following apply (mark all that apply)?

In the form of a ‘yes’ or ‘no’ question, Question 30 asked respondents if they believe uploading information from a CSD to a secure storage location is required by NJDOT or Division Policy. Of 57 respondents, 33 (58 percent of the total) indicated ‘yes’, while 24 (42 percent of the total) indicated ‘no’. Question 31 asked the same thing as Question 30, except in relation to vendor contract agreements. In this case however, most respondents, over two-thirds of which, did not believe this was required.

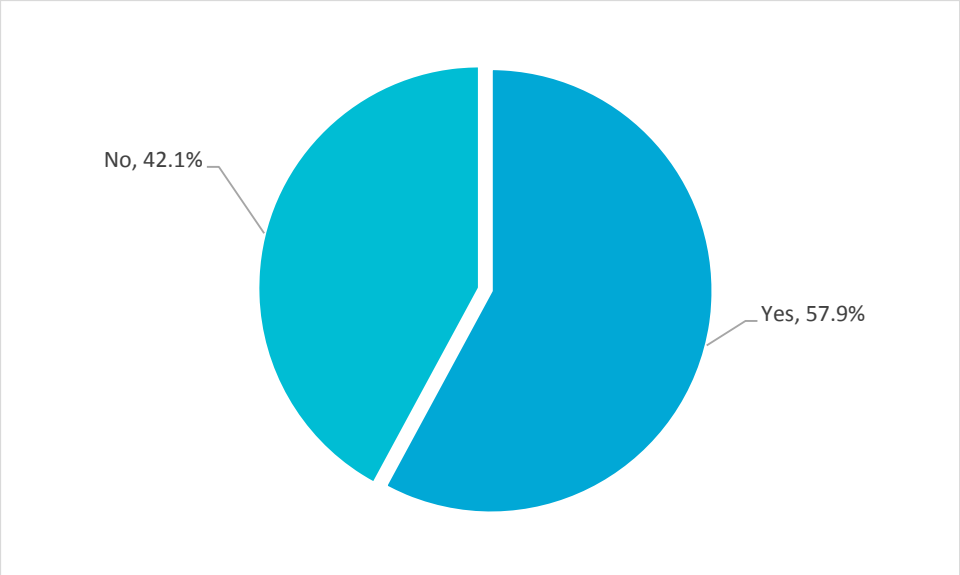

Figure 17. Question 30: Do you believe uploading information from a CSD to a secure storage location is required by NJDOT or Division policy?

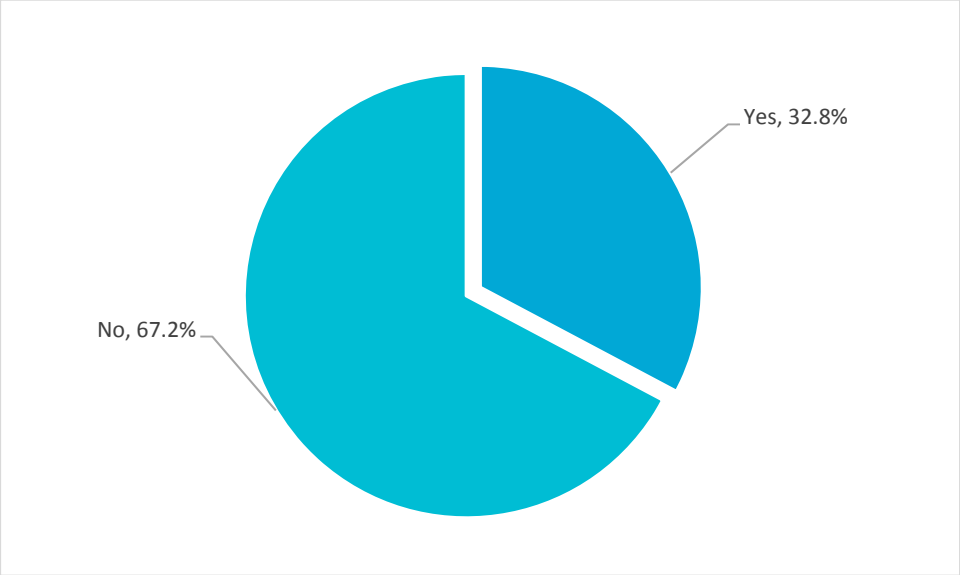

Figure 18. Question 31: Do you believe uploading information from a CSD to a secure storage location is required by vendor contract agreements?

Email Use Question Results

Question 32 asked respondents if they access any email accounts on a CSD. Out of 57 responses, 48 (84 percent of the total) indicated that they did access email. Only 9 (16 percent of the total) indicated that they don't do so.

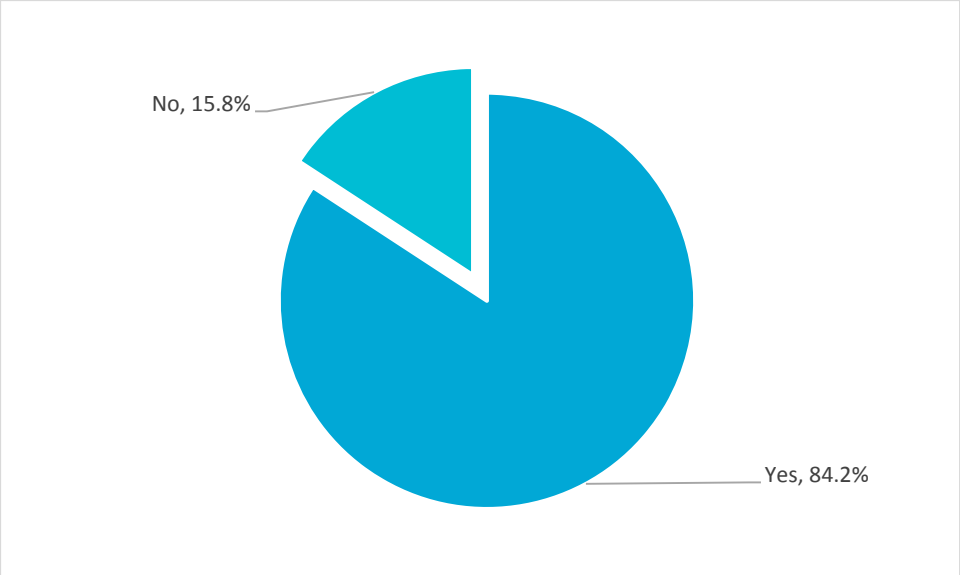

Figure 19. Question 32: Do you access any email accounts on a CSD?

Given that most respondents access email on a CSD, Question 33 asked respondents which emails they access. Respondents were allowed to select multiple responses as needed. Based on 66 responses, 100 percent of indicated that they access their NJDOT email address. Just over 20 percent indicated that they access their personal email address. About 10 percent indicated that they access a shared NJDOT email address related to a specific unit or project, while just 4 percent indicated that they access email addresses provided by state vendors, suppliers, consultants and/or contractors.

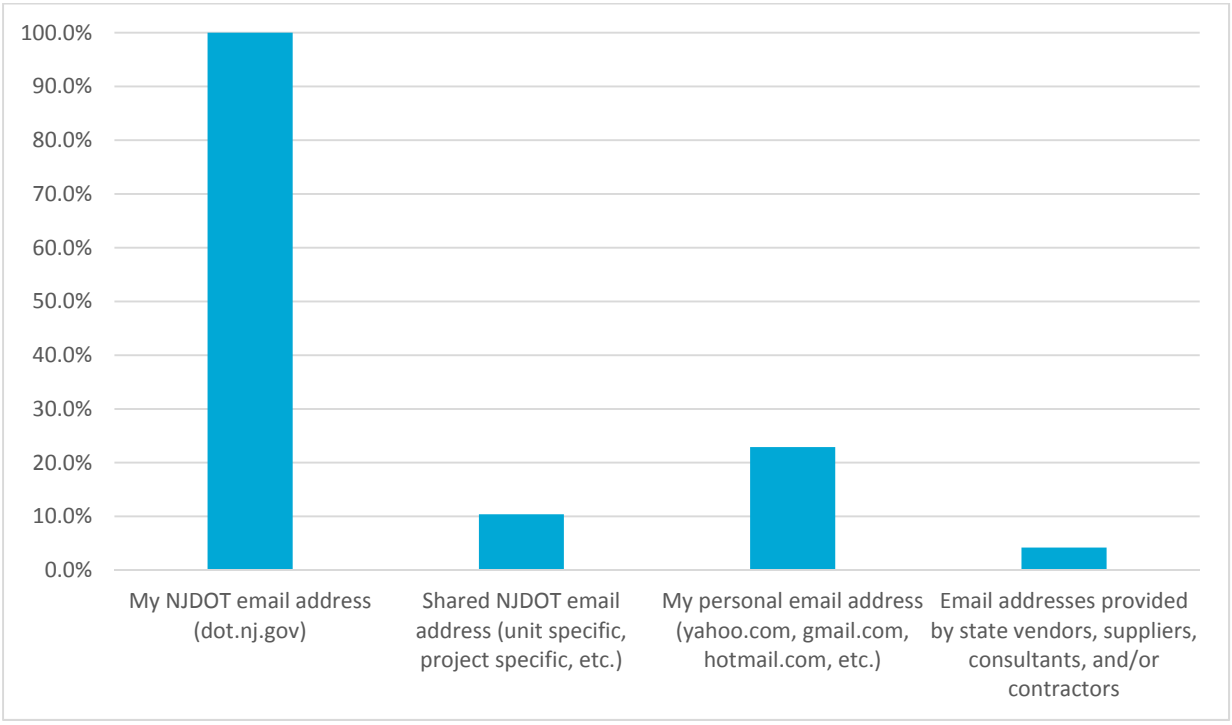

Figure 20. Question 33: Which email do you access on a CSD (check all that apply)?

Question 34 asked respondents how they access their NJDOT email on a CSD. Exactly half of respondents indicated that they used some sort of web browser. The next most popular response was via Microsoft Outlook or other similar application directly on the device, at 40 percent. The remaining 10 percent was split amongst 'Go to My PC' and via Microsoft Outlook or other similar application that had to be configured onto the device.

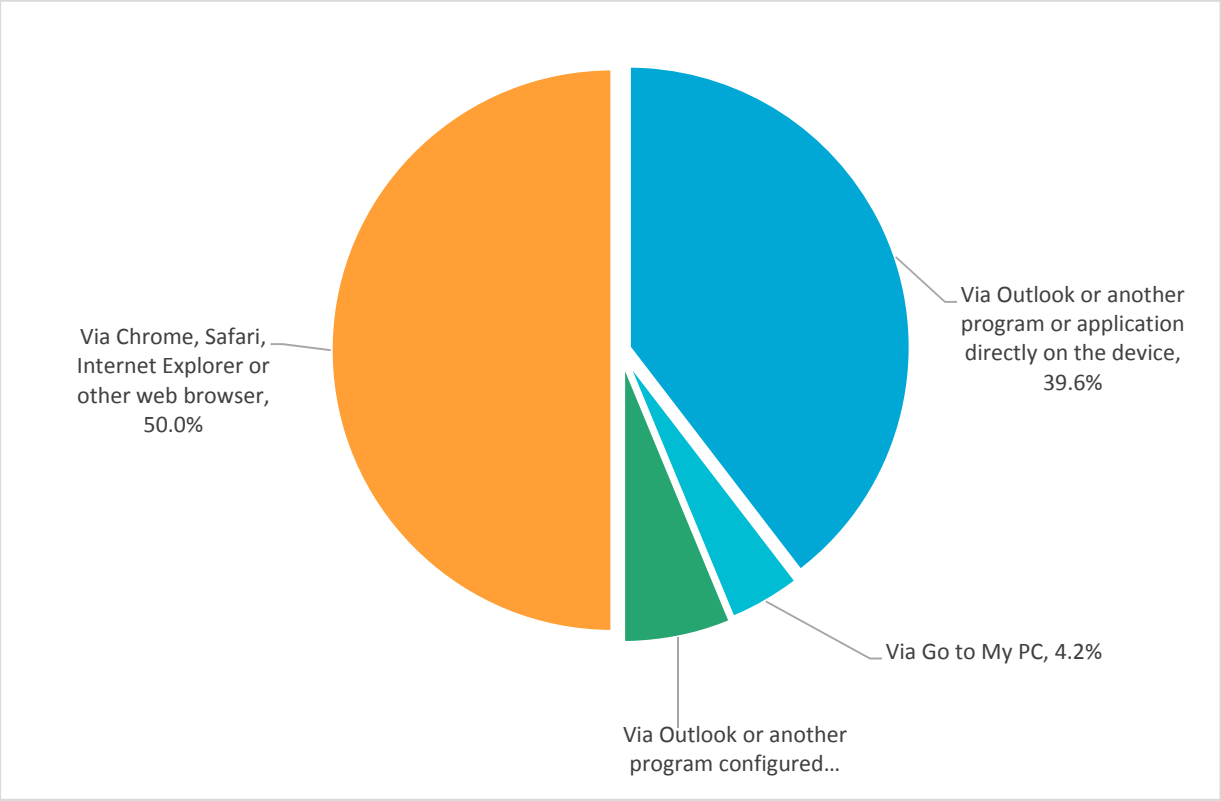

Figure 21. Question 34: How do you access your NJDOT email on a CSD?

Similar to Question 33, Question 35 asked respondents which email they access on an NJDOT device. Respondents were allowed to select multiple responses as needed. Out of 48 responses, 92 percent indicated that they access their NJDOT email address. Only 1 respondent indicated that they access their personal email address, while 3 indicated that they do not access any email on their CSD. There may have been an error in the final possible response, in that Question 35 asked about NJDOT devices, rather than CSDs.

Question 36 asked respondents if anyone has access to and/or uses any of the email accounts they use on an individually assigned CSD. Over 80 percent indicated that no one else has access. At a total of 9 percent, some respondents indicated that others have access to a shared NJDOT email address only. The remaining responses incorporated access by means of a vendor, supplier consultant, or other contractor.

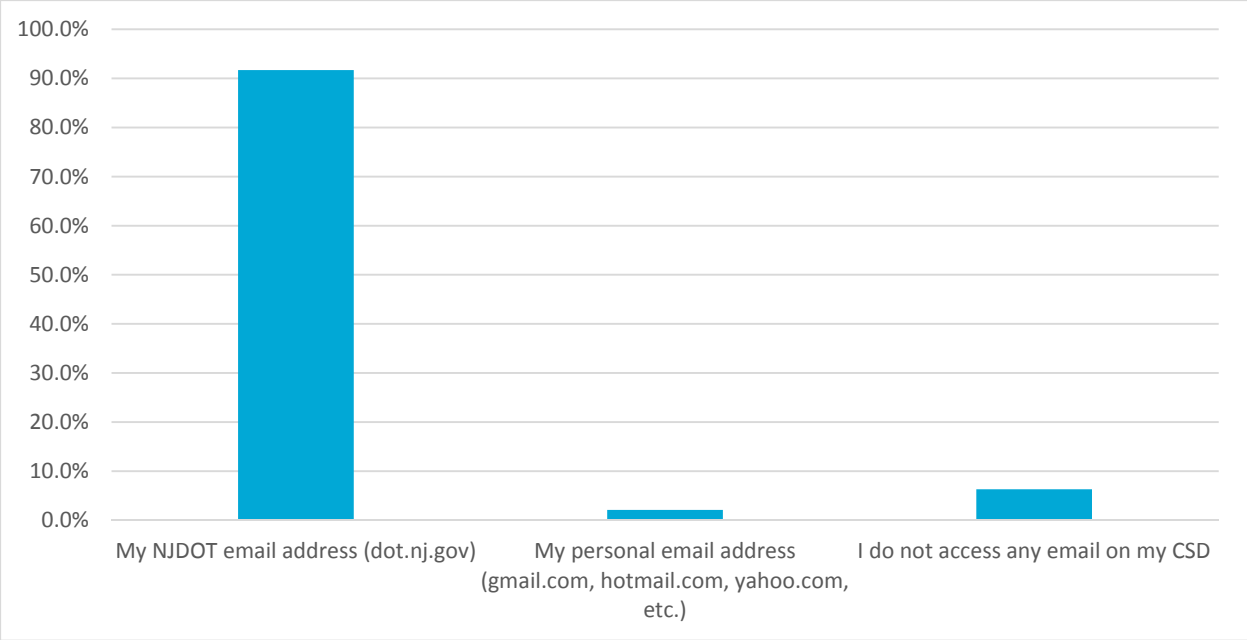

Figure 22. Question 35: Which email do you access on an NJDOT device (check all that apply)?

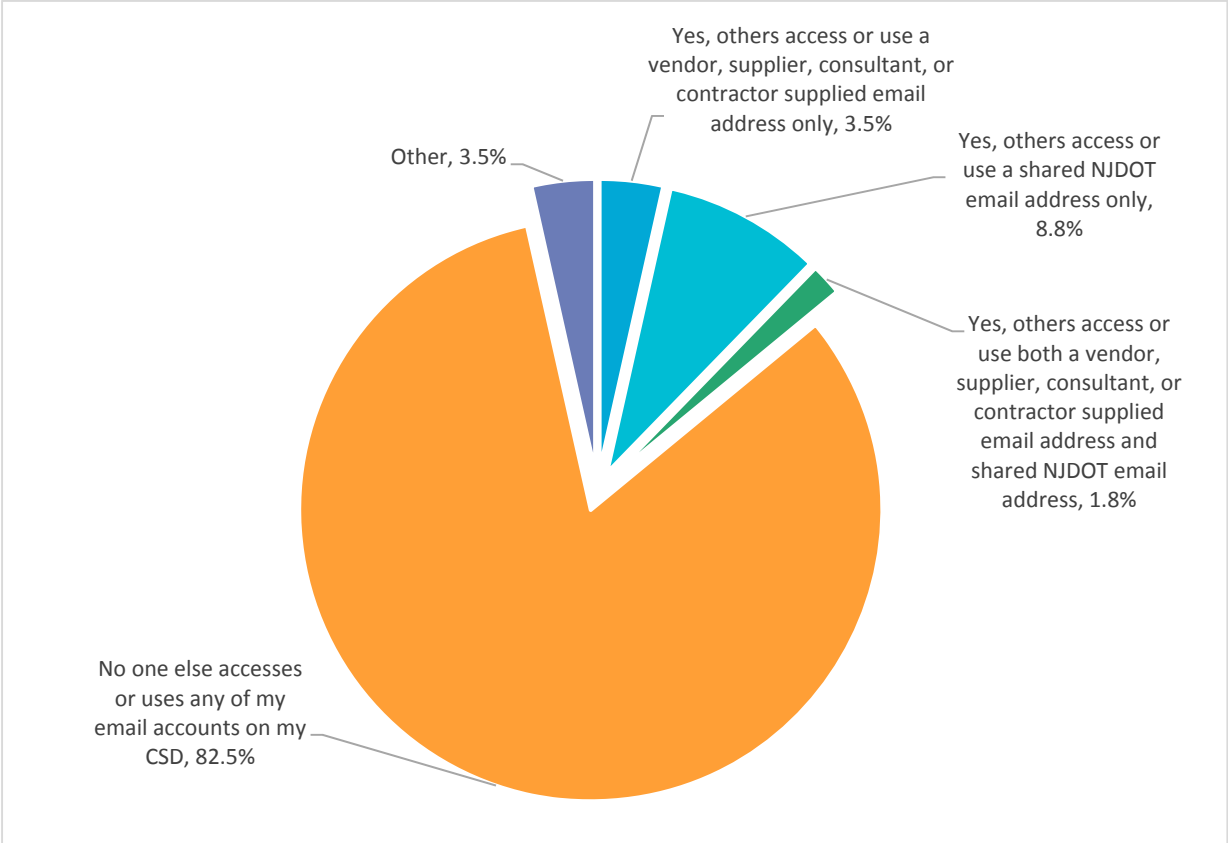

Figure 23. Question 36: Does anyone else have access to and / or use one or more of the following email accounts on your individually assigned CSD?

Question 37 asked respondents who has access to their CSD supplied email account from their CSD. Just over 75 percent of respondents indicated that no one else has access, while 12 percent indicated that another NJDOT employee has access. The remaining responses incorporated access by means of a vendor, supplier, consultant, or other contractor.

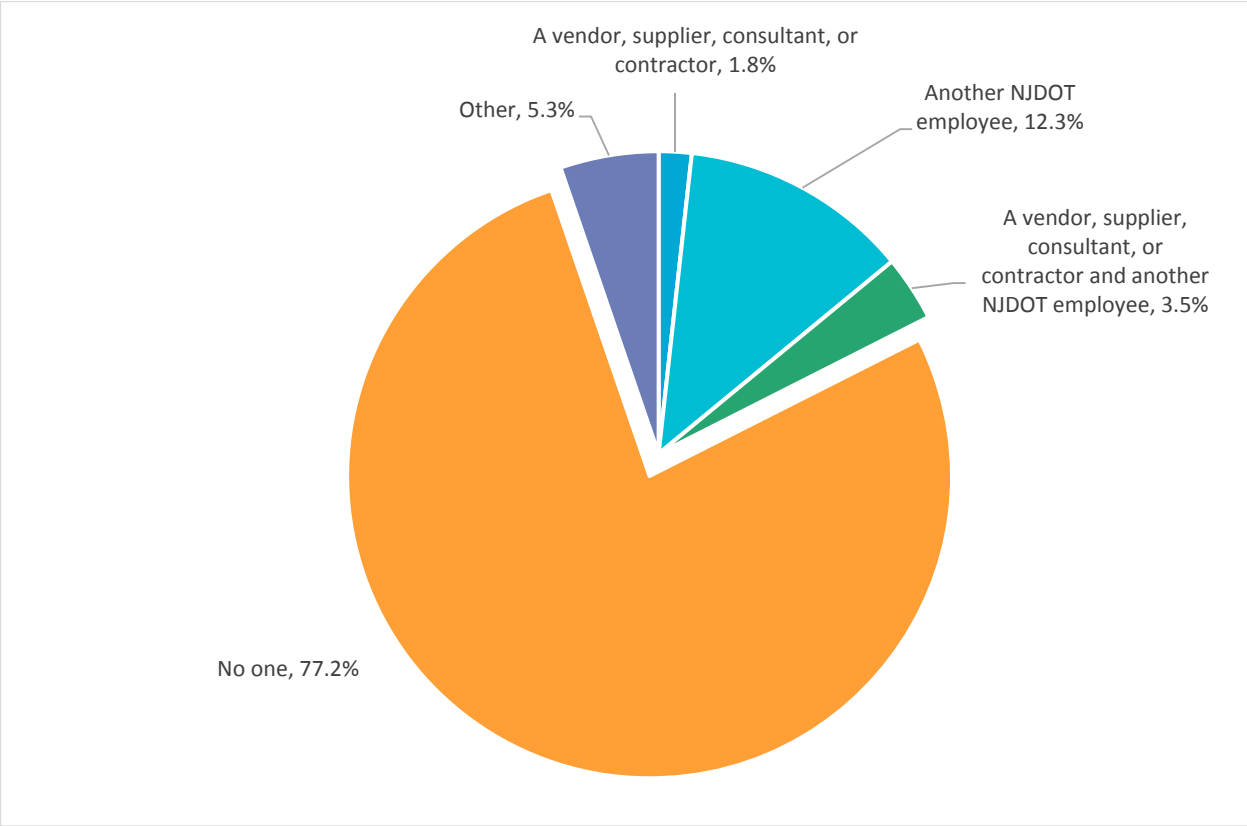

Figure 23. Question 37: Of the following, who has access to your CSD supplied email account from your CSD?

Following Up Question Results

To finish up the survey, Question 38 asked respondents if they could be contacted for follow up questions regarding their experiences with CSDs. out of 55 responses, 11 indicated that they could be contacted, while 44 indicated that they couldn't.

Question 39 asked respondents to list their contact information, and will be available via an excel database.

Lastly, Question 40 asked respondents to share additional thoughts about their experiences with CSDs and NJDOT policies governing the use of CSDs. Those open-ended comments provided by respondents are listed below:

- "All devices should be NJDOT devices not CSD"

- “Beneficial since the newest technologies are being utilized and not several years old, especially when handling more modern software such as AutoCAD, primavera, etc.”

- “CSD is economical as the cost of equipment and program are part of the project cost under the office set up and maintenance. The Contractor is responsible for maintenance of all supplied equipment within 24 hours and so far no issue on service.”

- “CSD's are unfortunately a necessary evil.”

- “Department needs to provide all field inspection a smartphone or tablet that can take pictures and videos for document work. When you have multiple inspector there are only one or two cameras per field office and the cameras are not available when needed. Consultant should provide their inspectors camera and computers. All the inspector should have a computer to write daily reports in circa 2017.”

- “First off, some of the questions in the survey required an answer, however none of the answers were correct for my situation but I had to pick one to continue, so some of my answers are not correct. Second, it would be far more convenient if my cell was supplied by the state because every time I change jobs, my cell phone and number changes and no one can reach me.”

- “I DO NOT KNOW”

- “I supervise a field office of about 12-15 staff (NJDOT and consultants.) By Contract, the Contractor supplies the office equipment. We use Outlook Web Access through the portal. Other than e-mail, site manger, crystal reports and the other NJPortal programs (ecats, epar), etc, we don't access NJDOT shared drives, FEMIS, etc. We don't seem to have any issues when using CSD for NJDOT work.”

- “Just have CSD's to be apple so the securities are better. No malware/virus”

- “My thoughts on the issue: Due to the nature of contractor supplied equipment for field offices; when it comes to laptops/desktops/printers/scanners and smartphones, the notion of a "man-in-the-middle" between NJDOT Field personnel and NJDOT Servers - the man-in-the-middle being the contractor - There is a level if uncertainty about who has permissions, credentials, etc. over that equipment/data. Given the spike of security breaches in recent times, these thoughts are heavy, and there is some level of discomfort. Field personnel occupy a unique digital space - forced to always use the portal - forced to explain to helpdesk "this is not a NJDOT supplied device that I'm calling about" Response "I can help you reset your password(s) but for systems issues you must contact the contractor's assigned IT representative and turn your device over to them for solutions"

- “Special Provisions need to require smart phones to allow email access and on the job research and access to links. It would also be beneficial to text photos.”

- “There should be a field tech for tech support and setup, similar to how there is a Site Manager support tech.”

- “Dealing with remote access is brutal at times, air card signal sporadic at best.”

- “It should be most modern device.”

- “Websense too restrictive on work-related videos sometimes incorporated into documents, presentations, and webinars.”

CONCLUSION AND RECOMMENDATIONS

In summary, this report has highlighted how CSDs utilized and managed in the general DOT work environment, as well as internally within the NJDOT.

This research effort was guided by the following key questions:

Where and how are CSDs deployed and what contractual mechanisms and what procedures are used to manage the acquisition, deployment and post-project disposition of CSDs?

CSDs are deployed throughout the DOT work environment, including within the headquarters, regional and field offices. This appeared to be the case in NJDOT, as well as the other DOTs that were contacted as part of the project. Those contractual mechanisms and procedures used to manage their acquisition, deployment and post-project disposition of CSDs vary however.

How are CSDs used by NJDOT staff to collect, manage and share information related to NJDOT projects and contracts?

Based on the survey results, NJDOT staff appear to use CSDs in the same manner as NJDOT-supplied devices. Within NJDOT, CSDs constitute to a wide variety of devices. This includes computers, tablets, drives, cellular and smart phones, and additional office devices including printers, fax machines, photocopiers and scanner. However, the majority of CSDs are computers (both laptop and desktop), followed by cellular and smart phones. The survey results additionally indicate that the frequency and commonality of CSD use does not vary by workplace setting or location either. While approximately half of survey respondents work out of the NJDOT headquarters, the other half are dispersed throughout other locations including regional offices and yards. In cases where NJDOT cannot supply necessary devices or technology, CSDs appear to be of an adequate substitute.

What data and information reside on CSDs?

How are data and information transmitted between the CSDs and NJDOT-controlled information systems and file servers while a project is in progress?

Based on the survey results, it was found that data transferring between CSDs and NJDOT devices does not occur frequently. In fact, over half of all survey respondents indicated that they do not actually move data between CSDs and NJDOT devices. Those respondents that do transfer data between the two types of devices tend to use thumb drives, or email, which tended to be the most common response. Additional methods of data transferring between the two types of devices included the use of a VPN, personal PC and CD or DVD burning. However, these additional methods are much less commonly used.

The variety in methods used to transmit data between CSDs and DOT-controlled information systems is further reflected in national trends. The use of email as a means of transmitting data is also a primary means for the Maryland Department of Transportation (MDOT), though MDOT also uses software packages when files become particularly large. Although Kansas Department of Transportation (KDOT) typically uses a VPN for these purposes, MDOT and North Carolina Department of Transportation (NCDOT) do not allow contractor devices to connect to VPNs. Additionally, although the use of CD and DVD burning to transmit information is less common within NJDOT, it is employed as a primary method by ODOT. These results indicate that there is currently no universally accepted method of uploading information between the two types of devices.

How are (and is) data and information stored on CSDs transmitted to and archived by NJDOT during the project close out process?

Note: None of the survey questions directly addressed this. Will leave this question open for further discussion with Chris/Brian.

Research Conclusions

CSDs are Necessary in the NJDOT Workspace

The use of CSDs is necessary in the NJDOT workspace as staff utilize these devices in the same ways that they utilize NJDOT-supplied devices. This can be attributed to limited supply and functionality of DOT-owned devices and the associated capital investments that would be needed to maintain an adequate supply. As a result, when managed properly, CSD use can be seen as a money-saving tactic.

Policies Governing Use and Management of CSDs Vary

Across other State DOTs, policies regarding the use and management of CSDs vary noticeably. For example, certain State DOTs prohibit VPN access to contractors and vendors, while other State DOTs allow this. There currently isn't a standardized best practices and recommendation guide for State DOTs to follow regarding CSDs.

Security Best Practices are Evident

Unlike other aspects of the use and management of CSDs, a review of existing policies revealed certain best practices in security. For those DOTs permitting contractor VPN access, they can allow access only to those softwares and projects needed to complete the project. Additional best practices include anti-virus software installment and enforcement, project close-out procedures and uniform security provision to all third parties.

Technical Support has not been Sought Often for Technology Devices

Most NJDOT staff have not needed technical support for technology devices, issued by NJDOT or independent contractions. For those staff that have sought technical support, those devices included desktops and laptops which were issued by both NJDOT and independent contractors. On the other hand, printers, fax machines, photocopiers and scanners required technical support in occasional instances from independent contractors.

Staff Does Not Have a Preference for CSDs over DOT-Supplied Devices

NJDOT staff do not have a preference for whether devices are supplied by NJDOT or a contractor. In those instances where NJDOT staff indicated that they had a preference for CSDs, it was attributed to the NJDOT not actually supporting or providing that type of device. If those devices were in fact supported or provided by NJDOT, staff would not have any issues using those devices.

Research Recommendations

Implementation of Security Best Practices. The research team recommends that NJDOT implement the identified security best practices regarding the use and management of CSDs. These best practices include restricted VPN access, enforcement of anti-virus software on all devices, project close-out procedures and uniform security provisions to all third parties.

Develop a Best-Practices Guide Entailing Best Practices for Transferring Data Across CSDs. Given a varying range of responses in relation to the methods used to transfer data across CSDs, the NJDOT should develop a best practices guide entailing prefer methods. The NJDOT should additionally further utilize software and cloud-based storage systems that will automatically sync data, eliminating the need for manual transfers on the part of staff and contractors.

Perform Economic Comparisons between NJDOT-Supplied and Contractor-Supplied Devices. Given the indifference amongst NJDOT staff as to which entity supplies needed devices and technology, NJDOT should perform an economic cost comparison to determine which method of supplying devices is more cost efficient. These cost comparisons should be conducted for each type of device and across multiple workspaces (headquarters, regional and field offices) to determine the most economically optimal solution regarding device supply and use.

IMPLEMENTATION

Based on the observations and findings of this research, it will be up to NJDOT to determine the best method for moving forward in the management of technological devices. Given that employees are primarily indifferent to the source of their devices, so long as they function properly, NJDOT should perform economic cost analyses to determine which, if any devices, NJDOT should supply and which should be relied upon through third parties, in order to reduce project costs without sacrificing time or craftsmanship. Once this is completed NJDOT can develop a plan specifying which devices are supplied through whom, while incorporating those identified best practices from other state DOTs.