

SOUTH CAROLINA



DEPARTMENT OF REVENUE

Equipping SC

a COVID Affected Workforce

Robert Franks

Contents

1. Problem Statement	2
2. Data Collection	4
3. Implementation Plan	8
4. Summary of Data	9
5. Summation	12
6. Bibliography.....	14
Appendix.....	15

1. Problem Statement

1.1. Background

The South Carolina Department of Revenue (SCDOR) is a cabinet agency. The purpose of SCDOR is “TOGETHER we are funding a better state to live, work, and play”. We directly and indirectly impact every aspect of the governance of South Carolina. Our work is essential to the continued health and well-being of our state, funding 95% of the state's general fund. [10]

Our mission is to administer and enforce the revenue and regulatory laws of the State with integrity, effectiveness, and fairness to all taxpayers, while maintaining the highest security and protection of taxpayer information. It is with this mission in mind that agency strategic goals are planned developed and implemented.

1.2. Department of Security and Technology Services

The purpose of the department of Security and Technology Services (STS) is “To equip people to excel by providing trusted technology and security services”. The Technology Services division, under STS, purpose is “To connect people through innovative solutions so that everyone can excel”. [10] These solutions include but are not limited to automation, Business intelligence (BI), Hyper-Converged Infrastructure (HCI) and cloud services. It is with those solutions in mind that STS works to ensure that not only our external customers can have reliable, efficient and secure platforms in order to conduct business, but our internal customer as well.

1.3. Problem Statement

When an emergency situation occurs, state employees should be amply prepared and have the proper resources to respond at a moment's notice. The problem with this statement is that not all state employees are employed by agencies that have the staff or resources to support this effort. This usually leads to various levels of disarray and frustration by employees. Management now have to improvise solutions without insight, and Agency Heads are left to deal with the aftermath of an ineffective workforce with limited availability to resolve. With issues reaching a national or even global level, available resources to resolve issues could either be unavailable or very expensive to purchase.

More expensive unique items that have not been purchased on a state level can be nearly impossible to procure. With the lack of necessary resources to effectively equip the state workforce, productivity as well as mass layoffs could be required. This has been proven with recent COVID-19 outbreak. Globally, lack of necessary resources as well as travel restrictions and regional quarantines has caused companies, both big and small, to close. Forced business shutdowns have led to record unemployment, exponential price increases and vital resource shortages.

This is why I believe that the state should proactively develop, test and implement strategies to equip a mobile workforce. By proactively developing solutions that will equip our workforce to be mobile; resources can not only be available for remote work, but more efficiently allow for agencies to find available resources in the event of an emergency. Also, by ensuring state employees not only have the necessary resources in the event of an emergency, agencies should know where to procure additional resources ahead of time.

In an ongoing effort to align with SCDOR Strategic goal 4 (Engage and empower employees). [10]

- Sub-goals 4.2 - Develop: Equip employees with essential skills, competencies and resources to succeed in their careers.
- Sub-goals 4.3 - Resources: Allocate financial resources to meet the needs of a developing workforce.

SCDOR is implementing a soft phone client for business continuity. SCDOR will utilize Segra Unify, a native Windows and Macintosh (MAC) client for unified communications. The software will allow users to continue assisting taxpayers and DOR staff under current circumstances due to COVID-19. Soft phone client will utilize current desk phone numbers and all calls will be routed to user's laptop or 2-in-1 (laptop and tablet) device via Segra Unify.

2. Data Collection

2.1. Background

In the beginning of 2019, the Technology Services division set out to equip a mobile workforce by deploying all laptops and 2in1 devices to all SCDOR employees. As a complimentary process to this migration, a near fully automated imaging process was developed that allowed hardware replacement to be completed in hours instead of days. Additionally, imaging carts were built to allow previously imaged, unassigned machines to stay on the network and up to date with latest patches minimizing deployment time. At the conclusion of these initiatives, management sought to implement other initiatives that would allow for a more mobile workforce. (Appendix A)

Keeping in line with the agency's strategic goal, it was recommended that we develop a plan that would allow SCDOR employees to able to access their desk phones remotely. This would not only allow for employees to receive office calls to their desktop, but also allow them

to make calls without having to distribute additional business cards or giving out personal numbers to customers. It was determined that our current carrier, Segra, had a solution that would meet the specific need without having to do a complete replacement of hardware.

(Appendix A)

2.2. COVID Impact

COVID-19 has proven itself to be a worldwide issue that is affecting multiple parts of the world similarly. According to a recent report by The World Health Organization (WHO) “the US, Brazil, India, and Russia are some of the worst affected countries due to the COVID-19 outbreak. The COVID-19 crisis has affected various industries worldwide in a negative manner and hence, the global economy is anticipated to face a slump in 2020 and 2021.” [3] This article goes on to narrate the increasing need for remote work and increased improvement of infrastructure to support this need. [3] The need for increased infrastructure is not limited to internal resources alone, virtual desktop computing has also seen a drastic comeback supplementing the need for more computing power without having to purchase or replace personal computers. Unfortunately, what this trend has also revealed is since most organizations store their data in a hybrid configuration, having some in the cloud while other portions remain locally, has required the need to still invest in a local physical footprint with an emphasis on network technology. The need for more resources has also led to businesses changing their computing strategy deploying strategies such as Bring your Own Device (BYOD) which would allow employees to utilize resources within their own homes to complete essential work tasks.

In addition to the horrific loss of life, the pandemic has led to unprecedented job loss. According to a report done by Congressional Research Services, the United States in April of 2020, reached unemployment rates greater than their highest unemployment rates during the Great Recession. During the pandemic, 31 percent of establishments (employing 68.6 million workers) increased telework offered to employees. In addition, 14 percent of establishments (employing 35.4 million workers) increased the amount of paid sick leave provided to employees.[2]

As indicated in a recent report by VMware, “more than two-thirds (67%) of government IT leaders indicate that they have expanded their Agile practices and continuous delivery (CD) methods in response to demands resulting from COVID-19”. [7] The Cybersecurity & Infrastructure Security Agency (CISA) also conducted a study in regards to supply chain readiness under COVID-19. Detailed below is an excerpt from the executive summary of the report...

“The COVID-19 global pandemic caused profound disruptions to the globalized model of supply chains, including those in the IT and Communication sectors. The global supply chain model constitutes sequential, multi-country production, where value is added in fragments along the way and where the country of origin is often difficult to determine. To that end, a product may be designed in New York, built in Vietnam, tested in Taiwan, stored in Hong Kong, and sent to China for final assembly, and distributed globally to end customers for use.”[9]

2.3. Testing

A Proof of Concept (POC) was developed and approved by management. Technical resources were identified and assigned to the project as well as a project manager. (Appendix A) Based on the information gathered, a set of objectives as well as a test plan were developed

to ensure that the solution would meet National Institute of Standards and Technology (NIST), Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) as well as Internal Revenue Service (IRS) Publication (PUB) 1075 requirements. [8]

In order to ensure that traffic utilizing the new software was encrypted from end to end, additional testing was required. Modifications to the application configuration file were implemented and tested. Routing modifications inside the SCDOR network were made for Session Initiation Protocol (SIP) traffic and tested. The use of Hunt groups / lines was also tested to ensure functionality for call center employees. Finally, after all testing was completed, the project process and configurations were reviewed by the Chief Information Security Officer (CISO) Team for Authority to Operate (ATO) approval. (Appendix B)

2.4. Monitoring

The technical staff wanted to be sure that their projections were close, so they decided to monitor the VPN traffic for bandwidth and percent processor utilized. Upon review of the first report, it was clear that more resources were needed. As more people transitioned to remote work, percent processor climbed to over eighty percent. Users were restricted to what they could perform over VPN. Some of the restrictions that were placed on users are as follows...

- No streaming of audio or videos
- No video conferencing except through agency portal (Skype)
- Utilize VPN during Office Hours (8:30AM – 5PM) unless your designated day for patching
- Do not leave VPN idle for more than 30 minutes

To ensure the current VPN concentrator was not overrun, the technical staff started to stagger user logins based on alphabet order. In addition to staggered logins, security patching also followed same concept as follows...

Steps to push the new VPN client and monthly updates:

- 1) Push the new VPN client by the Alphabetic order @ 2pm.
Instructions for step 1:
They will be disconnected from VPN. Reboot is recommended to connect to VPN again.
- 2) Push the monthly updates to the same collection on the same day @11:00pm.
Instructions for step 2:
Leave the laptop connecting to the VPN whole night, once patches apply it reboots the machine and it may disconnect you from VPN.
- 3) Following day they will get the new VPN client script once they connected to the network.
Instructions for step 3:
It will disconnect you from the VPN. Reboot is **REQUIRED** to connect to VPN again.

These measures allowed for all remote users to stay online for core functions while work was being conducted to put upgrades in place. (Appendix E)

3. Implementation Plan

3.1. Implementation

As the technical staff were wrapping up the POC portion of the project, news began to spread about the potential of sending state employees home due to the recent publicized COVID outbreak. Management teams began to assemble to determine what would be needed to send employees home, how quickly could these resources be gathered and distributed and what tasks or functions could not be performed remotely.

As the technical team developed a deployment plan for softphone technology, they quickly realized that the existing bandwidth and Virtual private Network (VPN) equipment would not

suffice to handle a near total remote agency staff. Understanding the need to not only handle VPN connectivity, but also external customers connecting to SCDOR web resources, the technical team determined that increasing internet bandwidth to one gigabit (1GB) while also upgrading existing F5 VPN concentrator would be the best solution to support the load.

Part of the team worked with Division of Technology Operations (DTO) which is a subsidiary of the South Carolina Department of Administration (SCDOA) to ensure the internet bandwidth increase was vetted and tested. Other portions of the team worked with third party vendors to procure the upgraded hardware ensuring that they were able to meet an extremely tight timeline. The remaining staff identified not only included call center staff that were part of the original scope, but all SCDOR staff members that required frequent access to their desk phone not only to receive calls which could have been handled with call forwarding, but also placing calls without revealing personal phone numbers to the public to conduct business. (Appendix C)

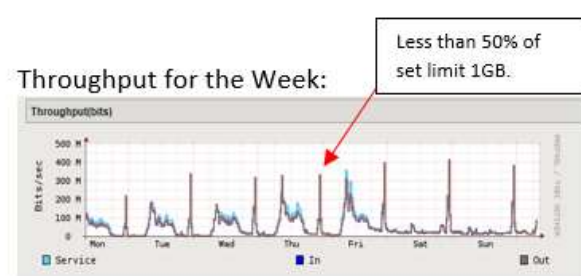
4. Summary of Data

4.1. Bandwidth Analysis

In order to ensure that our users could simultaneously access agency resources reliably, we determined that we would need to significantly increase our internet bandwidth. The bandwidth need could roughly be estimated by the type of data transmitted. There is a clear difference in whether utilizing 1 byte of data to configure hardware over Telnet protocols and using over 1K bytes to access an internal application. Essential functions such as making a

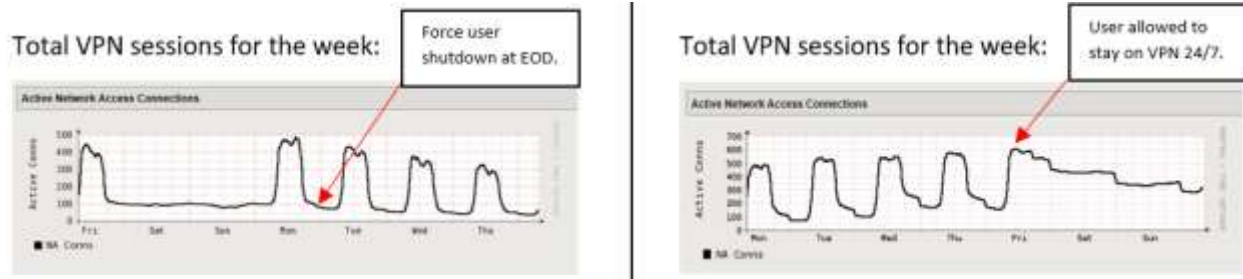
phone call over Voice over IP (VoIP) can add up quickly causing circuit overrun and possible outage. [5]

The technical team ran weekly reports and monitored the circuit throughout the day. As you can see from the chart below on the left, unmanaged use of the VPN tunnel caused over utilization of our subscribed 100MB circuit. Users were restricted on use and how long they could connect. Once more robust hardware was installed and bandwidth was increased to 1000MB, users were given unlimited access to agency resources allowing for flexibility and improved processes. (Appendix E)



4.2. User Analysis

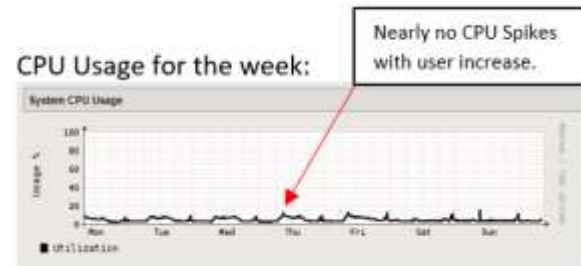
With near to a fully remote staff, it was important to allow core function to work while setting boundaries on basic infrastructure use. Numbers that were gathered confirmed that in order to achieve basic processes such as patching and compliance checks, strategic login strategies were needed. After implementation of the new hardware, users were allowed to utilize VPN without restrictions as seen in the graph below. (Appendix E)



As indicated by the number of users utilizing the VPN tunnel, the implementation of allowing users to work remotely was successful. The cooperation of staff as it relates to ensuring machines are utilized and online during assigned times for software updates in the initial deployment allowed technical staff time to stage and implement upgrade hardware. Open communication as well as active self-reporting when remote issues arise allowed management and technical resources to respond more efficiently. (Appendix F)

4.3. CPU Analysis

The VPN technology being utilized by the SCDOR runs the VPN server in a virtual shell, allowing multiple servers to run simultaneously performing various tasks (Load Balancing, VPN, etc.) while utilizing available memory and compute. With the additional load placed on the hardware due to COVID-19, the technical staff determined that hardware replacement would be required. The original equipment was never provisioned to handle the unexpected load requested of it. As with other resources required for VPN, user restrictions were put in place to accommodate load. Extra consideration was placed on ensuring that no matter future obstacles may arise, the VPN hardware was prepared to sustain. The chart below shows the CPU load placed on the VPN hardware before and after replacement. (Appendix E)



5. Summation

5.1. Strategic Plan

As outlined within this document, flexible and direct strategic planning as it relates to ensuring proper resources in the event of crisis is essential for remote work. This does not mean that all consumables need to be on the shelf or within grasp of agency consumers, however, knowing what, how and how long to acquire resources is vital towards determining which items need to be procured and in what order. In the paper, I have described how strategically testing softphone technology as well as aggressively implementing increased bandwidth and VPN upgrades, helped our agency speed up equipping our agency staff to be able to effectively work remotely. (Appendix C)

5.2. Hardware Availability

The success of getting agency staff working remotely was heavily driven on the availability of hardware to support decisions made by agency management based on the impact of global pandemic COVID-19. References given in this document indicates that acquisition of IT resources have been and will most likely continue to be a challenge moving forward. As indicated within this document, continued communication with hardware vendors as well as allocation of funding will be needed in order to be prepared for future challenges.

There isn't one right answer and no one has a crystal ball that can accurately predict the future; however, doing nothing in today's climate can have a rippling effect that could be felt throughout our cities, states and country. The best way to feed an economy is with an actively engaged workforce capable of being flexible and able to be productive wherever the office may be. There are multiple paths technology directives can take having their pros and cons. Each option must be weighed based on business needs and thoughtfully plotted towards amply equipping our workforce remains healthy, engaged and empowered.

6. Bibliography

[1] Unemployment Rates During the COVID-19 Pandemic: In Brief

<https://fas.org/sgp/crs/misc/R46554.pdf>

[2] Effects of COVID-19 Pandemic on the Employment Situation News Release and Data

<https://www.bls.gov/covid19/effects-of-covid-19-pandemic-and-response-on-the-employment-situation-news-release.htm>

[3] Impact of COVID-19 on the Virtual Desktop Infrastructure (VDI) Industry 2020-2027 - Demand from IT & Telecom Sector Amid COVID-19 Anticipated to Drive Growth

<https://www.globenewswire.com/fr/news-release/2020/08/17/2079060/0/en/Impact-of-COVID-19-on-the-Virtual-Desktop-Infrastructure-VDI-Industry-2020-2027-Demand-from-IT-Telecom-Sector-Amid-COVID-19-Anticipated-to-Drive-Growth.html>

[4] Virtual Desktop Infrastructure Market Forecast to 2027 - COVID-19 Impact and Global Analysis by Offering, Deployment, Enterprise Size, End User; and Geography

[https://www.researchandmarkets.com/reports/5136071/virtual-desktop-infrastructure-market-forecast-to?utm_source=GNOM&utm_medium=PressRelease&utm_code=vsfhm3&utm_campaign=1426470+-+Impact+of+COVID-19+on+the+Virtual+Desktop+Infrastructure+\(VDI\)+Industry+2020-2027+-+Demand+from+IT+%26+Telecom+Sector+Amid+COVID-19+Anticipated+to+Drive+Growth&utm_exec=joca220prd](https://www.researchandmarkets.com/reports/5136071/virtual-desktop-infrastructure-market-forecast-to?utm_source=GNOM&utm_medium=PressRelease&utm_code=vsfhm3&utm_campaign=1426470+-+Impact+of+COVID-19+on+the+Virtual+Desktop+Infrastructure+(VDI)+Industry+2020-2027+-+Demand+from+IT+%26+Telecom+Sector+Amid+COVID-19+Anticipated+to+Drive+Growth&utm_exec=joca220prd)

[5] Managing VPN bandwidth requirements, speed and overhead

<https://searchnetworking.techtarget.com/answer/What-is-the-bandwidth-utilized-on-Internet-VPN>

[6] What is a VPN Concentrator and How does it Work? - Stephen Mash

<https://www.privacyaffairs.com/vpn-concentrator/>

[7] [Report] MIT Technology Review Insights Survey Reveals Government IT Trends Impacted by COVID-19 Pandemic

https://blogs.vmware.com/industry-solutions/2020/12/15/mit-technology-review-8-government-it-trends/?src=sp_5fd8c8369043e&li_fat_id=8c460889-7797-466c-94e8-c64d4ea4c362

[8] IRS PUB 1075

<https://www.irs.gov/pub/irs-pdf/p1075.pdf>

[9] BUILDING A MORE RESILIENT ICT SUPPLY CHAIN: LESSONS LEARNED DURING THE COVID-19 PANDEMIC

https://www.cisa.gov/sites/default/files/publications/lessons-learned-during-covid-19-pandemic_508_2.pdf

[10] SCDOR Purpose and Mission

<https://dor.sc.gov/about>

Appendix A

Soft Phone POC Test Plan

Project Name:	Soft Phones POC Test Plan
Request Number:	J86E69117A
Date:	1/28/2020
Project Sponsor(s):	Dale Brown
Project Requestor:	Robert Franks
Project Manager:	Charita Cato

Document Approval

- A.** The following is the list of mutually agreed upon individuals needed to sign this document to consider it approved:

Name	Title
Matthew Calder	Business Analyst
Samantha Jeffries	Security Analyst
Robert Franks	Infrastructure Manager
Marjorie Kneece	PMO Manager
Christopher Barhorst	CTO
Alex Jackson	CISO Manager
Dale Brown	CIO

- B.** By signing below, the signee certifies that this document has been reviewed and signed by all parties, or person delegated to sign on behalf of a party as stated in **A** of this section.

X

Document Purpose

This document serves as the test plan for this initiative. The goal of this document is to guide the testing process, laying out the various testing scenarios, testing dates, and the resources who will perform the testing. This will help to ensure technical and business objectives are met with a specific focus on business needs, technical design, security compliance, system performance, etc.

High-Level Test Objectives

1. Ensure criteria meets current and future requirements.
2. Ensure Agency compliance and security requirements are met and tested accordingly.
3. Ensure the new environment has high performance rates with thorough performance testing.
4. Ensure there is a non-disruptive migration strategy through proper testing.
5. Ensure Customer Support expectations are met or exceeded.
6. Ensure testing strategy supports requirements of SCDOR.

Scope of Test

- Testers will have software installed on their workstations
- Accounts will be created for the client
- Testing will take place over 1 week
- All cases will be tested over wireless and VPN

Testing Team

Name/Dept.	Role
Karen Hildebrand	Call Center Manager
Ty Onley	Telecom
Charita Cato	PM
Tina Brown	Networking
Sean Perry	Networking

Testing Schedule / Resources / Status



[Test plan Matrix](#)

Revision History

Revision #	Revision Date	Section Revised	Revision Description	Updated By
1.0	1/4/2020	Document Created	Created initial document	Charita Cato
1.1	1/22/2020	Test Matrix	Updated test matrix	Charita Cato
1.2	1/28/2020	Test Plan	Updated testing team	Charita Cato
1.3	1/29/2020	Test Plan/Matrix	Updated approvers and test cases	Charita Cato

Appendix B

Soft Phone POC ATO Checklist

Project Manager: Charita Sumpter Security Analyst: Samantha Jeffries [TRB Sharepoint Link](#)

TRB Project Name: Softphone POC

CAB I-Support Ticket #s J8DH453122

Change Control: Date Criteria & Timing 1st Established for the Project

Dates Criteria & Timing Updated:

List IP Addresses:

Security Criteria	Timing of Security Review	Current Status DATE UPDATED:	Notes
Variances and Exceptions Approved	4	Status: complete Date Approval Completed: 3/16/2020 Variance/Exception #s:	Sam
Zero Unpatched Vulnerabilities	4	Status: complete Date Approval Completed: 3/16/2020 Variance/Exception #s:	Sam
Zero Outstanding Compliance Findings (STIG / SCSEM Hardening, Manual SCSEMs, FIPS 140-2)	4	Status: complete Date Approval Completed: 3/16/2020 Variance/Exception #s:	Sam – Voice Video Endpoint STIG and VOIP SCSEM
Firewall Review	4	Status: complete Date Approval Completed: 3/16/2020	Sam
Access Review	4	Status: complete Date Approval Completed:	Mari
SIEM Logging Verified	4	Status: complete Date Approval Completed: 3/26/2020	Liz
Anti-Virus Verified	4	Status: complete Date Approval Completed: 3/26/2020	Liz
HX Verified	4	Status: complete Date Approval Completed: 3/26/2020	Liz
Software Whitelisting Verified	4	Status: complete Date Approval Completed: 3/16/2020	Sam
Security-Related Tests Completed	4	Status: complete N/A Date Approval Completed:	
Submit new or updated Disaster Recovery plan	4	Status: N/A Date Approval Completed:	Not needed for POC
Other security criteria specific to the system: [Add rows]	4	Status: complete N/A Date Approval Completed:	

LEGEND: Security Review Timing

- 1 = System is in build environment. ATO security review # 3 is required before system is moved to final environment.
- 2 = System is in its final environment. ATO security review # 3 required before system is put into operation.
- 3 = System is in its final environment and is in operation before ATO security review # 3, due to the nature of the system (e.g. a core network device). ATO security review # 3 is required immediately after system is operational.
- 4 = System is in POC environment. ATO security review #3 is required for POC before Production TRB#2.

Clarifications (as needed):

Documented Evidence / Collateral (Embedded here CM-3 / Bridge Diagram / etc etc):

Appendix C

Agency Email of New Features Implemented

From: Communications & Strategic Solutions <Communications@dor.sc.gov>
Sent: Wednesday, April 29, 2020 12:36 PM
To: DOR <DOR@dor.sc.gov>
Subject: VPN upgrade and other important news

Good afternoon,

As you may have heard, on Monday Governor McMaster issued [Executive Order 2020-29](#) to extend the state of emergency and allow the state's response to COVID-19 to continue. We are continuing to follow the guidelines set by the Governor and will provide updates to you as they become available. Please stay connected to agency news by following [The Huddle](#) and staying in close contact with your supervisor as we all adjust to this new, but temporary, normal.

We have exciting news to share with you as we make the most of this difficult situation. Last week we successfully deployed important VPN updates to the agency. As a result, our remote working capabilities have increased, including:

1. **Enhanced video capabilities** – The restrictions on watching videos while working remotely have been removed. You are now free to use Skype video conferencing, LinkedIn Learning, and other work-related training videos using your SCDOR device.
 - Learn more about activating your LinkedIn Learning account and other remote training opportunities [here](#).
 - *Tip: Use Internet Explorer to watch videos on LinkedIn Learning!*
 - Please limit your audio or video Skype meetings to no more than 75-80 users at a time.
2. **Stay connected to VPN all day** – You no longer need to log on and off of VPN to preserve capacity. The designated login times in the morning between 7:30 AM – 9:30 AM based on last name no longer applies, and you should login according to your normal work schedule (unless otherwise directed by your supervisor). You are encouraged to stay logged on to VPN throughout the day and leave your machine connected overnight. Make sure to continue to follow your designated patching schedule. Learn more in the updated [Telecommuting Resource Guide](#).
3. **Expanded and more reliable softphone service** – The new VPN can support the hunt lines on softphones more reliably, resulting in additional phone service capacity and fewer dropped calls. To find out which phone lines are available to serve customers again, see the updates [posted in this article](#).

View other important updates, including new dos and don'ts of working remotely, in the [Telecommuting Resource Guide](#). Continue checking [The Huddle](#) every day to stay connected with agency news.

If you have any questions about using VPN while working remotely, contact the [HelpDesk](#).

Thank you to everyone involved in developing and implementing these enhanced VPN capabilities. Thank you to all of the SCDOR team for your continued commitment to serve South Carolinians.



Communications & Strategic Solutions






803-898-5201 | Communications@dor.sc.gov

South Carolina Department of Revenue | dor.sc.gov

The content of this email and any attachments may be confidential and legally protected from disclosure. If you are not the intended recipient of this email, please reply immediately to notify the sender, then delete it from your system. You are prohibited from sharing any part of this message with a third party.

Appendix D

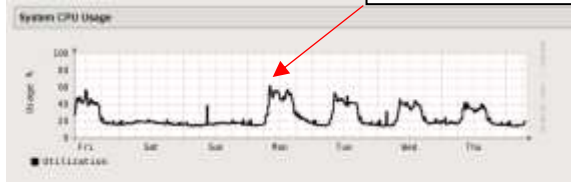
Softphone Test Plan

Category	User/Technician	Test Case	Requirement No.	Requirement	Expected Results	Completion Date	Tester	Actual Results	Complete/Not Complete	Collateral	Notes
Hardening and Scanning	Technician	DOR Security Standards	SR-4	Solution will meet the CISO requirements as defined within DOR Security standards (i.e., PCI, PUB 1075 / SCSEMs, DISA STIG, and DOR CISO Security Standards). The technician will provide evidence in support of completion of tests to meet compliance.	Solution meets the CISO requirements as defined within DOR Security standards (i.e., PCI, PUB 1075 / SCSEMs, DISA STIG, and DOR CISO Security Standards). The technician has provided evidence in support of tests to meet compliance.	2/21/2020	Samantha Jeffries	PASS	COMPLETE		
Hardening and Scanning	Technician	Other Hardening Guides required by CISO		Solution will meet the CISO requirements as defined within specified hardening guides. The technician will provide evidence in support of completion of tests to meet compliance.	Solution meets the CISO requirements as defined within the specified hardening guides. The technician has provided evidence in support of tests to meet compliance.	2/21/2020	Samantha Jeffries	PASS	COMPLETE		
Hardening and Scanning	Technician	FIPS Settings	SR-1	The overall solution will be FIPS 140-2 Level 1 compliant.	The vendor solution adheres to FIPS 140-2 Level 1.	2/21/2020	Samantha Jeffries	PASS	COMPLETE		
	Technician	Nessus Scanning		Nessus scanning and hardening will take place by default across any new component on the network. Root access to the device is highly preferred but not required. The technician will provide evidence in support of completion of tests to meet compliance.	Solution will not have any compliance/vulnerability issues. The technician has provided evidence in support of tests to meet compliance.	2/21/2020	Samantha Jeffries	PASS	NOT COMPLETE		
Reporting and Monitoring	Technician	Logging		Ability to view access logs to include call history	NOC/SOC able to see logs for login and call history	2/21/2020	David Thompson	PASS	COMPLETE		
Hardening and Scanning	Technician	DOR Security Classifications	SR-2	Solution will incorporate the standard DOR and security data classifications of FTI, STI, PI, etc.	Solution incorporates the standard DOR and Security data classifications of FTI, STI, PI, etc.	2/21/2020	Samantha Jeffries	PASS	COMPLETE		
User Functionality	User	Call Transfers	UR-18	Ability to transfer calls within client	Solution is able to transfer calls from one line to another.	2/7/2020	Testers	PASS	COMPLETE		
User Functionality	User	Conference Calls	UR-19	Ability to perform conference calls	Solution is able to perform conference calls.	2/7/2020	Testers	PASS	COMPLETE		
User Functionality	User	Call Forwarding	UR-20	Ability to perform call forwarding	Solution is able to forward calls to another line.	2/7/2020	Testers	PASS	COMPLETE		
User Functionality	User	Voicemail Forwarding	UR-21	Ability to transfer perform voicemail transfers	Solution is able to transfer voicemails from one voicemail box to another.	2/7/2020	Testers	PASS	COMPLETE		
User Functionality	User	Call Mute		Ability to place call on mute.	Solution allows ability for user to place call on mute.	2/7/2020	Testers	PASS	COMPLETE		
User Functionality	User	Internal Calls		Ability to make and receive internal calls.	Able to make and receive internal calls.	2/7/2020	Testers	PASS	COMPLETE		
User Functionality	User	External Calls		Ability to make and receive external calls.	Able to make and receive external calls.	2/7/2020	Testers	PASS	COMPLETE		
User Functionality	User	Listen to Voicemail		Ability to listen to voicemails.	Ability to listen to voicemails.	2/7/2020	Testers	PASS	COMPLETE		
User Functionality	User	Manage Voicemail		Ability to manage voicemail.	Ability to manage voicemails.	2/7/2020	Testers	PASS	COMPLETE		
	User	Land line to Soft Phone		No additional work required to switch from land line to soft phone	No work other than user signing in to Sepura Unity is required to switch from land line to soft phone	2/7/2020	Testers	PASS	COMPLETE		
	User	Number of users on client		Numerous users can utilize soft phone client simultaneously	Numerous users are able to use soft phone client simultaneously	2/7/2020	Testers	PASS	COMPLETE		
Feature Management	User	Login/Logout (Call Center)		Ability to login/logout of hunt lines	Users has the ability to login/logout out of assigned hunt lines	2/7/2020	Testers	PASS	COMPLETE		
Feature Management	User	Roll Over No Answer (RONA) (Call Center)	UR-1	Agency hunt lines will maintain the "roll over no answer" function.	Solution is able to perform "Roll Over No Answer".	2/7/2020	Testers	PASS	COMPLETE		
Feature Management	User	"Kill" Codes (Call Center)	UR-2	Maintain the ability to use agent id codes to "kill" the agency phones lines	Solution is able to use Agent ID codes to "Kill" agency phones lines	2/7/2020	Testers	DEFERRED	N/A - KILL CODE PROCESS WILL NOT BE DONE THROUGH CLIENT		
Feature Management	User	AUX Codes (Call Center)	UR-14	The AUX Codes should be accessible (Break, Lunch, Supp/Approv, Meeting, Other Duty, Assist, Personal, Training)	Allows for use of AUX Codes	2/7/2020	Testers	PASS	COMPLETE		
Feature Management	User	Announcements (Call Center)		All announcements must play correctly from the main menu.	All Announcements play correctly from the main menu.	2/7/2020	Testers	PASS	COMPLETE		
Feature Management	User	Call Tree (Call Center)		Maintain current call tree	Current call tree is maintained in the client	2/7/2020	Testers	PASS	COMPLETE		

Appendix E

VPN Weekly Metrics Before and After Upgrade

CPU Usage for the week:



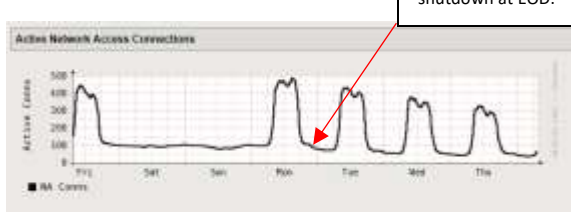
High CPU Spikes with user increase.

Throughput for the Week:



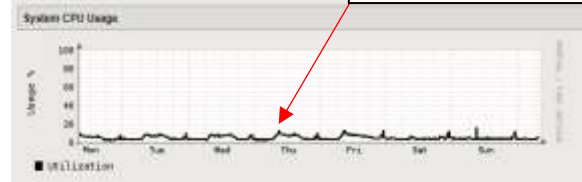
Over Bandwidth set limit 100MB.

Total VPN sessions for the week:



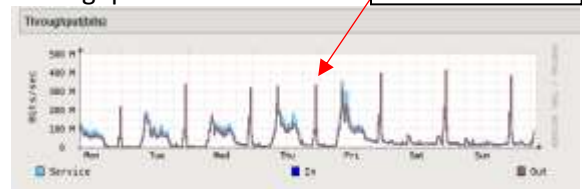
Force user shutdown at EOD.

CPU Usage for the week:



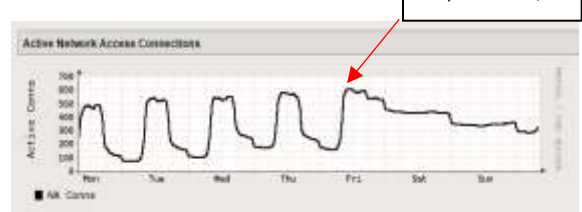
Nearly no CPU Spikes with user increase.

Throughput for the Week:



Less than 50% of set limit 1GB.

Total VPN sessions for the week:



User allowed to stay on VPN 24/7.

Appendix F

Call center Best Practices for Remote Users

Best Practices from the Call Center

1. Maintain normal work routine.
2. Sign in 5 – 10 minutes before time to make sure your internet and VDN is working properly if not restart your system.
3. If it is still not working call the helpdesk.
4. Make sure you are in a quiet area with no TV or other distractions.
5. If possible don't work in your bedroom unless you have desk or a table you can work off.
6. Try your best to be focus and consistent with your task.
7. Make leadership aware of any problems you are experiencing at that time. (Email, Skype, or Text)
8. If you don't have the answers to the questions have the taxpayers to email the sections directly if you are unable to transfer the call.
9. Note the account accurately for the next person.
10. If call drop, please try to call taxpayer back to assist them.
11. Remain calm and don't get frustrated because we are all in it together.
12. Understanding – this is a difficult / adjustment for everyone, and having understanding to your employees' home circumstances are very essential.
13. MOTIVATION / ENCOURAGEMENT – Continue to motivate and encourage your team daily. Let them know you recognize & appreciate their hard work and dedication. It goes a long way when others feel appreciated, their encouraged, and get that daily motivation. It also boost their morale while working from home 😊
14. Communication – always be available for your staff whether it be through Skype, email, cellphone, etc. (Remember they are taking calls and assisting taxpayers. They still have questions and need assistance. It is very frustrating to them, when the taxpayer has to hold for long periods of time when they are trying to reach out to leadership for assistance & are not able to reach anyone)
15. Checking-IN – Remember to check on your employees and team throughout the course of the day. Send emails or Skype to see how their call volume is flowing, monitor Broadsoft and be sure if you haven't received any calls in a long period of time to check your connection.
16. Sign on to the system at least 15 minutes early. This will give you time to ensure you are connected and ready to take calls
17. When signing onto Segra Voice, make sure you are available within the call center
18. Read, Read Emails
19. Make sure you are in private area of home
20. Communication is essential, skype and email constantly, do not assume anything.
21. Show patience and compassion this is something new for everyone and this is stressful
22. Pace yourself
23. Monitor the phone system frequently
24. Make sure your environment is conducive to working, no distraction can give the callers your undivided attention.

25. Take your 2 -15 min breaks and 1 hour lunch, working from home is a little harder and will need to regroup and stretch.