verizon✓

# A Proposal to

# State of West Virginia

for

## RFP for Managed and Hosted Voice Services (OT18027)

## Volume 1. Technical Proposal

## Original

**November 27, 2018**

**Presented by:**
Sandra Hawkins
Sr. Client Executive

4700 Maccorkle Avenue
Charleston, WV 25304
304-356-3395
sandra.k.hawkins@verizon.com

verizon✓

Verizon Enterprise Solutions
4700 Maccorkle Avenue
Charleston, WV 25304
Phone: 304-356-3395

November 21, 2018

State of West Virginia
Department of Administration, Purchasing Division
Attn: Mark Atkins
2019 Washington Street, E
Charleston, WV 25305

To State of West Virginia:

Thank you for giving us the opportunity to present our proposal.

By choosing to partner with Verizon you receive secure, reliable, and flexible services that enable you to deliver your key business programs and provide the control and predictability you seek. Our products and services will help you bring the future to your customers.

Our value-based proposal addresses requirements from a business, financial, technical, and operational perspective. Our solution leverages:

- Configurable technology platforms that provide the foundation to build solutions to help overcome your business challenges.
- Industry innovation and solutions to meet existing and evolving requirements.
- Robust scale and flexible options for delivery and management.
- Vendor ecosystems, enabling us to create and deliver end-to-end business, communications, and industry solutions.
- Highly skilled teams of professionals.

We are committed to State of West Virginia's success. We sincerely appreciate your consideration and would be honored to continue to provide State of West Virginia with services that provide better business results, better experiences, and better peace of mind. If you have questions, please contact me at 304-356-3395 or via email at sandra.k.hawkins@verizon.com. I look forward to engaging with you and your team.

Sincerely,

Sandra K Hawkins

Sandra K. Hawkins
Senior Client Partner
304-356-3395

# Contents

# General Information

## Nature of Proposal

This RFP response is submitted to the West Virginia Purchasing Division on behalf of West Virginia Office of Technology (referred to herein as "Customer") by Verizon Business Network Services Inc. on behalf of its affiliate, MCI Communications Services, Inc. d/b/a Verizon Business Services (individually and collectively referred to herein as "Verizon").

Notwithstanding anything to the contrary contained in the RFP documents, Verizon does not consider this RFP response as legally binding to provide the Services described herein until all exceptions have been resolved, a mutual understanding is reached, and a contract is executed.

As permitted in the WV Purchasing Division's Procedures Handbook, Section 7.2.19, Verizon also submits additional terms and conditions reflected in Verizon's Service Agreement, which is incorporated and included in Verizon's response.

Verizon has included a signed WV-96 and understands Verizon's terms and conditions shall not supersede the WV-96 terms and conditions where a conflict arises.

## Pricing Disclaimer

Verizon pricing is based upon the set of requirements for the services set forth in the RFP. In the event Customer alters those requirements, or third party charges change, Verizon pricing may change.

The prices set forth in this Response exclude the following: (a) taxes, tax-like charges and tax-related surcharges; (b) "Governmental Charges" as defined in the Guide; (c) other charges expressly excluded by the final agreement to be negotiated between the parties; and (d) other charges published in the Tariffs and/or Guide.

## Validity Period

Unless otherwise stated in this proposal, this proposal is valid for a period of ninety (90) days from the date submitted.

During this period, promotions may expire and rates, charges, and/or discounts may fluctuate with changes in the Tariffs or Guide unless specifically stated as fixed in this proposal.

## Subcontractor

If subcontractors are to be involved in the provision of services contemplated in this RFP response, this RFP response and any resulting agreement are dependent upon Verizon being able to negotiate commercially reasonable underlying agreements with such subcontractors.

## Assumptions

1. Verizon assumes that Customer does not require bidders to administratively manage any contracts Customer has directly with third parties.

2. Verizon assumes that all services are expected to invoice from the bidder US to a Customer US entity at a US address.

3. Verizon assumes that any contract will be between two entities incorporated in the United States.

4. Verizon assumes that Customer will have no objection to a non-US affiliate executing a separate Master Agreement for any services provided by a Non-US bidder affiliate to a non-US Customer affiliate.

5. Verizon assumes that Customer agrees to comply with all export regulations and restrictions of any jurisdiction in which services are provided.

6. Verizon assumes that Customer will keep all bidders or bidder affiliate information provided in response to this RFP confidential to the same or greater degree it would protect its own information of the same or similar type.

7. Verizon assumes that Customer understands that for tax, regulatory or possible export restrictions, that Service Order Forms may need to be executed between entities of a country where CPE or a service involving labor is delivered. Please indicate any disagreement with this assumption.

8. Invoicing and Billing: Verizon assumes that invoices will be generated by and sent to the contracting parties (which may be the contracting parties to a country-specific Service Order Form or similar schedule submitted pursuant to the master agreement) at an address in the country in which the contracting party is organized.

Verizon will consider alternatives which it will review and approve subject to system capability, tax, regulatory and vendor/subcontractor issues.

9. CPE and CPE Related-Services: CPE and CPE-related services (including but not limited to installation and maintenance) will require execution of Service Order Forms or similar paperwork, in the country where the CPE will reside or CPE-related services are performed.

# Executive Summary

The State of West Virginia, through the Office of Technology provides vital administrative and technology services to enable West Virginia's reinvention.

The primary purpose of your RFP is to present a unified communications platform to all State of West Virginia agencies and allow for rapid adoption of new, best-in-class technologies and features. In order to achieve this, we will strategically partner with the State of West Virginia to help you deliver your technology-enabled vision.

We are pleased to provide a proposal in response to your invitation to bid. We have included our approach which leverages Strategic partnerships and investments we have made in emerging technologies so that the benefits can be directly passed onto you.

We Understand Your Challenges. Today, constituents, like never before, are expecting convenience and ease when dealing with their government. They are expecting more options to engage government, including digitally and online. At the same time, they still hold government to be good stewards of the taxpayer dollar.

This has created an ever-increasing pressure to:

- Create a “Constituent 360” environment, where the constituent engages via their preferred channel and loses no service quality
- Increase Channels of constituent engagement
- Steward the taxpayer dollar by Trimming costs
- Enhance organizational agility to respond to constituent needs
- Improve the ability to innovate

Communications excellence is a pillar to addressing these new challenges in the public sector, and this requires government leaders to explore new solutions and trusted partners to achieve the goal. West Virginia recognizes this and takes this important step via this RFP.

In your RFP, you mentioned some key aspects of your current state (significant data points bolded and underlined):

“The State presently uses a varied collection of infrastructure, equipment, and services to support the diverse communications needs of the State. These services have historically been supported by a dedicated group of internal State staff.

The envisioned strategic direction is to leverage a single Contractor-provided Voice over Internet Protocol (VoIP) service, and provide reliable, efficient, secure, scalable, and cost-effective managed voice, unified communications and contact center services to the State.

## Our Proposed Solution

Succinctly and concisely this paragraph provided us the drivers for our solution. Verizon combined several services into a comprehensive solution for the State to meet these drivers. The highlights of these services are detailed below.

Verizon sees the most important priority as taking over management of your existing Cisco IP telephony infrastructure. Verizon proposes to do this in partnership with TEKsystems.

Verizon proposes to utilize the existing two contractors the State uses today as onsite support. Their day to day knowledge of the current environment will ensure a smooth transition as management is transitioned from the State to Verizon.

These two onsite resources will be backed up by a knowledgeable Service Desk and technical resources to provide round the clock support for the State's users. They will also be invaluable as the State transitions from an onsite solution to a hosted one.

Verizon anticipates that the Standard Security Hosted Voice solution will meet the needs of most users. At its core, this is the same technical platform as your current UCCaaS users use today.

However, it is provisioned under a new contracting platform that allows access to improved features. This provides UC&C services such as call control, integrated/unified voicemail, presence and Instant Messaging, and enterprise mobility, integrated with Cisco Webex and Verizon audio conferencing.

By delivering these core Unified Communications (UC) services from its secure, state-of-the-art data centers, Verizon is able to provide and manage UC&C capabilities using a subscription-based monthly billing model.

The core Hosted Calling services are based on Cisco's Hosted Collaboration Solution virtualized application portfolio, providing customers with the security benefits of dedicated applications and the convenience and cost benefits of a hosted environment.

Verizon has expanded its partnership with Cisco, and now co-markets and co-sells with Cisco worldwide. Verizon partners with Cisco to maintain and provide operational support services for hosted voice.

Verizon also supports integrated Cisco cloud UC offerings, such as WebEx (Web conferencing) and Cloud Connected Audio (audio conferencing). Verizon also continues to expand the hosted voice offering with its wireless voice over Long Term Evolution (VoLTE) service.

Verizon's expanded partnership with Cisco enables customers to scale and upgrade quickly when HCS platform upgrades are available. Verizon has been able to take advantage of new APIs integrations for its customers including Salesforce and Service Now.

## Benefits

Hosted Unified Communications services help organizations achieve the following objectives:

- Access to the full set of sophisticated UC features available with advanced premise-based solutions – Organizations can benefit from the feature richness and integration flexibility typically associated only with premise-based solutions.
- Access to comprehensive management support – With Hosted Calling, customers receive a range of fault management, configuration management, asset management, and performance management services, with customized, built-in security practices—without having to develop full internal expertise typically required with a premise-based solution.
- Trade capital expenditures for predictable monthly expenses – Costs of the UC Platform hardware and software, implementation, maintenance, upgrades and ongoing management are accounted for by a recurring monthly fee based on the number of users.

  This better matches costs with actual needs, and smooths out the budget impact typically associated with one-time capital expenditures from premises-based equipment.
- Control costs while maintaining customization and flexibility—Organizations benefit from the usage-based pricing structure of cloud computing infrastructure and environments, while maintaining the custom integration and version/patch flexibility of a premise-based solution
- Introduce collaboration capabilities across the company – Companies can provide common tools between mobile and desktop, helping achieve faster response times from workers and speed critical decisions and processes.
- Upgrade TDM or IP PBX systems and control costs – Customers can replace the high cost call routing, equipment maintenance and Move, Add, Change and Delete (MACD) expenses with the cost control opportunities available through hosted IP Telephony.
- Extend unified communications into sites that do not have current generation IP PBXs.

  IT staff can provide regional and branch offices and remote workers not covered by the company's IP PBX network with unified communications without the capital outlay of an IP-PBX purchase or the IT support management these deployments require.
- Anytime/any device access to Unified Communications applications.
- Voice: IP phone, Single Number Reach or Mobility features, Extension Mobility, Cisco Jabber Desktop clients, and Jabber Mobile clients for smart phones or tablets are available and provide the same user experience regardless of device type.
- Messaging: Traditional Phone Telephone User Interface, IP Phone Cisco View Mail, Mobile Phone Voice View, Jabber clients, Microsoft Outlook Integrated Messaging, or Webmail, are available and no matter the device the messaging experience is the same.

- Integrate unified communications with third party business-critical applications, services, and platforms.
- Through the Jabber Software Development Kit (SDK), there are numerous opportunities to integrate Hosted Calling with third party applications, services, and platforms.
- Improve productivity by leveraging unified communications with business-critical third-party services.

While this is a very secure solution, the State identified the need for a subset of users to use a higher security solution.

Unified Communication and Collaboration as a Service (UCCaaS) for Government is Verizon's hosted and managed high security service also based on Cisco's Hosted Collaboration Solution (HCS). It was built from the ground up to meet stringent FedRAMP security standards.

It is completely separate from the Standard Security platform descried above. However, the services provided and support model is similar. Verizon hosts more than 100,000 Public Sector users today.

## Security Excellence

Verizon takes a specific approach to communications security that is important to understanding our solution. Often times communications providers apply a data security approach because it is the most common paradigm in security discussions.

At Verizon, we understand the nuances of communications security. The first thing to understand is the most common focus of security threats is not necessarily the communications itself. Rather, it is denying the communications.

We call it T-DOS, telephony denial of service, and it is a very real threat. This is not to suggest that intrusion is not a motive, because it is also a threat. However, a balanced security approach understands the full spectrum of security and puts capabilities in place to address those.

Verizon's security solution addresses the full spectrum of concerns. From denial of service to hijacking communications to actually trying to listen in, Verizon has a solution for them all. We are continually ranked as the most advanced company in security in the telecommunications sector by Gartner, and our solutions reflect this.

Aside from the features and the technology, the most important aspect of our solution is that it utilizes the Verizon network (please see the figure below). This is critical, as Verizon is one of the largest and most secure networks in the world.

Our culture of partnership extends our communications network to far reaching places economically and seamlessly enabling West Virginia to have confidence in its communications even in the most niche use cases.

UCCaaS (Unified Communication and Collaboration as a Service) for Government is FedRAMP (The Federal Risk and Authorization Program) compliant.

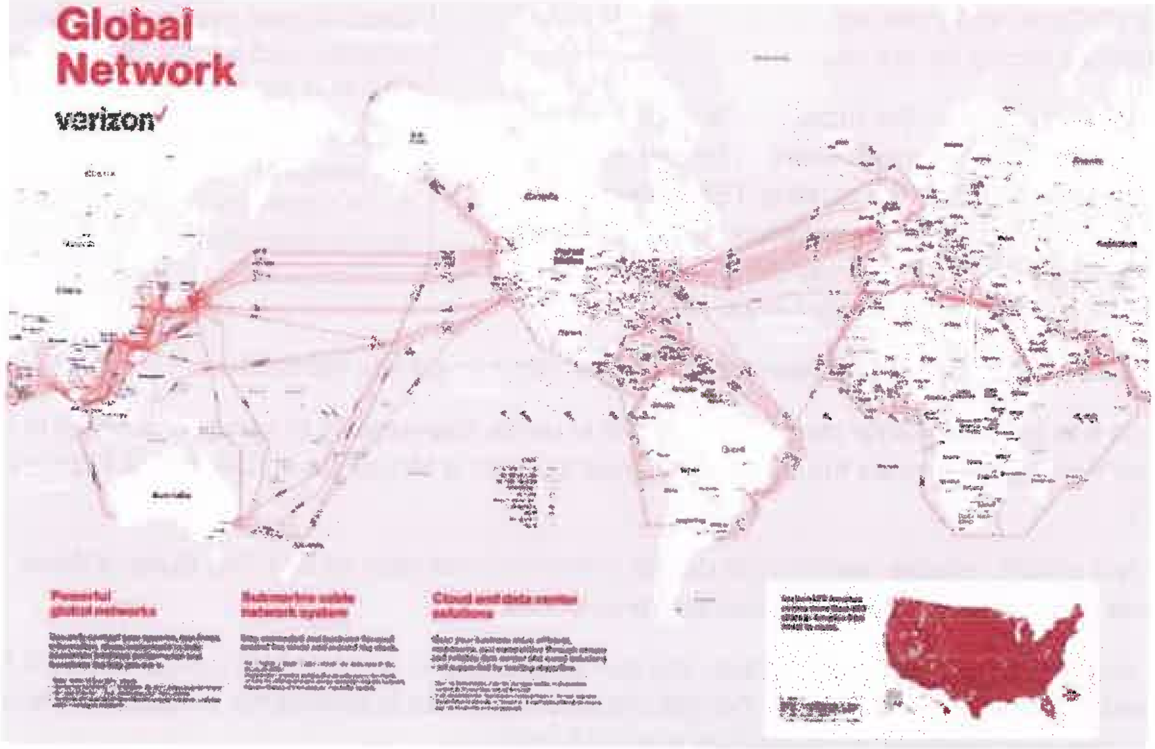
FedRAMP processes are designed to assist federal government agencies in meeting Federal Information Security Management Act (FISMA) requirements for cloud systems.

By standardizing security assessment, authorization, and continuous monitoring for cloud products and services, this program delivers costs savings, accelerated adoption, and increased confidence in security to U.S. government agencies that are adopting cloud technologies.

UCCaaS for Government security features include:

- FISMA compliant through FEDRAMP
- Dedicated Per-Customer Application Deployments
- Comprehensive Encryption of Sensitive Data
- Continuous Monitoring
- Application Based Policy Enforcement Management
- Third Party Reviews and Audits

Most notably, it is hosted in the Verizon Network which is heralded annually by independent organizations as one of the more secure in the world.


Global Network
verizon
Australia
Powerful global networks
Submarine cable network system
Cloud and data center solutions

*The Verizon global network.*

The powerful combination of Verizon's network-based services and Cisco's Unified Communications platform, together with Verizon's professional consulting expertise, helps enable better organizational processes and productivity for our clients while assembling the building blocks to provide cloud-based unified communications as a service.

We are a Cisco multinational certified partner is the U.S., Canada, and countries throughout EMEA and APAC.

We are a Cisco Gold Certified Partner in the U.S., United Kingdom, Germany, Netherlands, Australia, Hong Kong, Philippines, and Singapore. We are a Cisco Silver Certified Partner in Canada and France.

As a Cisco Gold Certified Partner with multinational certifications, we are part of an elite group of providers with proven in-depth technology skills and customer success in selling, deploying, and providing services for Cisco solutions.

In addition to technology advantages, being a Cisco Gold Certified Partner provides Verizon with access to a broad range of Cisco resources, as well as providing competitive pricing for our customers.

One of the challenges the State has faced is collecting the data necessary to move users to hosted voice. Verizon plans to utilize the existing TEKsystems contractors to lead the data collection effort with user agencies to speed up the transition from the existing on-premises platform to the hosted ones.

**UCCaaS for Government through the Verizon & Cisco Relationship**

The Verizon UCCaaS for Government offering is based on the virtualized Cisco HCS platform.

Verizon has expanded its partnership with Cisco, and now co-markets and co-sells with Cisco worldwide.

Verizon partners with Cisco to maintain and provide operational support services for the UCCaaS for Government platform.

Verizon also supports integrated Cisco cloud UC offerings, such as WebEx (Web conferencing), CMR (video), and Cloud Connected Audio (audio conferencing).

Verizon also continues to expand the UCCaaS for Government offering with its wireless voice over Long Term Evolution (VoLTE) service.

Verizon's expanded partnership with Cisco enables customers to scale and upgrade quickly when HCS platform upgrades are available.

Verizon has been able to take advantage of new APIs integrations for its customers including SalesForce and Service Now.

The State also asked for an option for small sites with non-private handoffs.

Verizon has two options for these sites. One is to utilize Expressway to securely connect to the Hosted Voice platforms via the Internet. A second option is Virtual Communications Express (VCE).

VCE is a simple, reliable approach to deliver critical technologies so that The State of West Virginia can confidently focus on business possibilities.

With Virtual Communications Express, you get an end-to-end communications service built for you and delivered from our cloud. You get phone service that is packed full of features that can help make your business more efficient and productive.

You get state-of-the art phones, specifically designed for businesses like yours. You get instant messaging and presence, audio and video conferencing, and desktop and mobile screen sharing that will enable you to collaborate internally and with your customers and suppliers better than ever before.

Virtual Communications Express is a robust, yet simple "plug and play" or professionally installed solution:

- Benefits and efficiencies of anytime unified communications capabilities across corporate voice and IT systems.
- Ability to boost productivity using existing broadband Internet service or Private IP connections.

  The State of West Virginia can use the collaborative and mobile tools that Virtual Communications Express offers – i.e. audio and video conferencing – to easily and quickly bring employees or clients together when making decisions.

  Mobile clients can also enable the ability to take calls and conduct conference meetings while on the go. You can remain productive when outside of the office (unlike plain old telephone service), and maintain continuity, so your business can continue to run smoothly.
- Alleviate the effort, complexity, and risk associated with technology management.
- Access leading applications and self-service capabilities.
- Simple installation and activation – no IT expertise required.
- Seamless communication across your organization, right "out of the box".

Virtual Contact Center is a complete cloud-based contact center solution providing the State of West Virginia with a comprehensive set of contact center tools, without requiring a costly investment in software, hardware, and support personnel. With this solution a you can provide agent training, properly schedule and staff agents, and interact with customers.

Virtual Contact Center allows an agency's customers to choose the method of contact most convenient to them. Customers can contact a business' contact center via phone, e-mail, SMS, social media, or the company's website. They can leave a voicemail, wait in queue for the next available customer service agent, or they can request a call back from an agent.

With the comprehensive set of routing options agencies can improve their customer's experience and increase first call resolution. Inherent contact reporting will provide the State of West Virginia with real time and historical reports ensuring the agencies are meeting their internal contact handling metrics.

Agents have at their fingertips access to e-Learning modules which will increase their knowledge when not handling inbound interactions. Supervisors can properly forecast and schedule contact center agents through embedded Work Force Management capabilities.

Key points of Virtual Contact Center Include:

- 100% Hosted in geographically redundant data centers
- Multimedia support including voice, e-mail, chat, SMS, and social media
- Integrate with 3rd party systems like Salesforce.com, Right Now, Microsoft Dynamics, or internally developed systems
- 99.99% Platform Uptime guarantee
- Global offering that can support Agent deployments in the U.S. and EMEA

Virtual Contact Center provides a comprehensive set of tools that will fit any opportunity. From the smallest new contact center to complex enterprise solutions, Virtual Contact Center will allow the State of West Virginia to provide exceptional customer service.

## Implementation Approach, Global Scale, and Flexible Options for Delivery and Management

The State of West Virginia RFP outlined Project Goals and Objectives that were expected of the selected partner to implement the new services. Verizon reviewed this in detail and has built our approach upon the request. This approach has been used in other enterprise deployments, and we are intimately familiar with it.

We deliver our services to provide scale, delivery, and management options thus providing you with the flexibility to invest in innovation, manage costs, and maintain operational controls in the proper balance for your organization.

We offer a range of delivery, management, and professional services engagements to create the flexibility you need to advance your organization.

Verizon has total confidence that we can address this initiative within your requested timeline. With that noted, our goal is to explore accelerating the migration and to shorten the legacy platform support window. This gives all locations the ability to utilize the unified communications platform earlier, thus enjoying greater productivity.

Verizon will leverage its professional services team to perform the work. This team is large and qualified with over 5,250 Cisco certifications within the group. They have experience in many implementations similar to this.

Their expertise will be critical to ensuring this initiative stays on schedule and delivers the benefits your users are expecting. Additionally, their collaborative approach ensures impact to State IT is minimized, and the project is delivered smoothly.

## Four Key Capabilities

You can count on us to be your trusted technology provider. Our approach comprises four key capabilities that, when combined, help your organization innovate and perform:

- Securely deliver information to more people and places with intelligent networks.
- Get the computing resources you need to make better, faster decisions with a dynamic cloud.
- Keep your employees productive, where and when they work, with workforce mobility and communications platforms.
- Connect with more customers — and more information — with connected machines.

Plus, our technology provides the underlying security solutions designed to protect your network, devices, and critical information.

## A Solution with Benefits Today and Tomorrow

In general, by choosing a Verizon solution, you can benefit from the following:

- Consistency. All services managed using the same standardized approach
- Visibility. Single global reporting environment; heavy use of data to generate insights for management
- Reliability. Rigorous meeting and document control, accurate inventory management
- Development. Commitment to continual service improvement and ongoing innovation
- Engagement. Interaction with users and executives thru regular forums
- Specifically, we help address your challenges and fulfill your objectives by:
- Hybrid Unified Communication Service
- Lower Total Cost of Ownership
- Faster, More Cost-Effective Deployments

## As the State of West Virginia's Strategic Partner, We Can Help You Transform Your Organization

In today's rapidly transforming environment, we design, build, and operate the networks, information systems, communication platforms, and mobile technologies that help businesses and governments around the globe expand reach, increase agility, and maintain longevity.

With our legacy of innovation and a proven ability to execute, we offer the technology platforms, industry solutions, global reach, vendors, and people necessary to create the specific solutions your enterprise needs.

Ultimately, we can help you harness the opportunities of the evolving advanced technology landscape, find new opportunities for your specific business goals, and reap the benefits of technology-led business transformation.

Recommendations and Next Steps. Based on what we currently understand of State of West Virginia's requirements, plus what we see in the marketplace, we look forward to the next step in the RFP process.

## Summary

By selecting Verizon as your solution partner, The State of West Virginia can leverage our adaptable technology platforms, expertise, experience, and innovation so you can continue to focus on your business.

- We're a trusted partner to the world's largest companies. Nearly all of Fortune 1000 uses Verizon technology and services.
- We're a communications service provider with a scale that few can match. We manage more than 4,000 customer networks and over 345,000 security, network and hosting devices.
- We have also made significant investments in the technologies that matter most to businesses today, including security, data centers, 4G LTE, cloud computing and our expansive global IP network.

We look forward to advancing our relationship and working together delivering exceptional services to your needs and in serving the constituents of West Virginia, now and in the future.

# Section 1. General Information

## *Cover Pages*

### Verizon Response

Please reference the Cover Page provided on the following page(s).

Purchasing Divison
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

**State of West Virginia**
**Request for Proposal**
**35 — Telecomm**

**Proc Folder:** 462803

**Doc Description:** RFP for Managed and Hosted Voice Services (OT18027)

**Proc Type:** Statewide MA (Open End)

| Date Issued | Solicitation Closes | Solicitation No | Version |
|---|---|---|---|
| 2018-08-29 | 2018-10-24<br>13:30:00 | CRFP 0212 SWC1900000001 | 1 |

**BID RECEIVING LOCATION**

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

**VENDOR**

**Vendor Name, Address and Telephone Number:**

Verizon Business Network Services Inc. on behalf of MCI Communications Services, Inc. dba Verizon Business Services
Sandra Hawkins
4700 Maccorkle Avenue
harleston, WV 25304
hone: 304-356-3395

**FOR INFORMATION CONTACT THE BUYER**

Mark A Atkins
(304) 558-2307
mark.a.atkins@wv.gov

**nature X** **FEIN #** 47-0751768 **DATE** November 20, 2018

**All offers subject to all terms and conditions contained in this solicitation**

**ADDITIONAL INFORMATION:**

The West Virginia Department of Administration, Purchasing Division (hereinafter referred to as the "Purchasing Division") is issuing this solicitation as a request for proposal ("RFP"), as authorized by W. Va. Code 5A-3-10b, for the West Virginia Office of Technology (hereinafter referred to as the "Agency") to provide Managed Voice Services for the State's Legacy VoIP Environment, while working to migrate those Legacy vironments to a Hosted VoIP Platform, included Hosted Contact Center Services per attached documents.

ɯANDATORY PRE-BID MEETING:
DATE: 09/26/2018
TIME: 2:30PM EDT
LOCATION: WV Office of Technology
1900 Kanawha Blvd. E.,
Building 5, 10th Floor
Charleston, WV 25305

NOTE: Online responses to this solicitation are prohibited. Please see the Instructions to Bidders in Section 2 for proposal submission.

| INVOICE TO | | SHIP TO | |
|---|---|---|---|
| ALL STATE AGENCIES<br>VARIOUS LOCATIONS AS INDICATED BY ORDER | | STATE OF WEST VIRGINIA<br>VARIOUS LOCATIONS AS INDICATED BY ORDER | |
| No City | WV99999 | No City | WV 99999 |
| US | | US | |

| Line | Comm Ln Desc | Qty | Unit Issue | Unit Price | Total Price |
|---|---|---|---|---|---|
| 1 | Managed and Hosted Voice Services | 0.00000 | EA | | |

| Comm Code | Manufacturer | Specification | Model # |
|---|---|---|---|
| 81161700 | | | |

**tended Description :**

ʖee Attachment_A Cost Sheet for proposal pricing.

Vendor shall use the Attachment_A Cost Sheet for proposal pricing.

Note: online proposal submissions are prohibited.

Please see Section 5 Vendor Proposal Subsection 5.3 for further instructions.

**SCHEDULE OF EVENTS**

| Line | Event | Event Date |
|---|---|---|
| 1 | Mandatory Pre-Bid Meeting @ 2:30pm EDT: | 2018-09-26 |
| 2 | Technical Questions due by 2:00pm EDT: | 2018-10-05 |

## ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

Purchasing Divison
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Request for Proposal
35 — Telecomm

**Proc Folder:** 462803

**Doc Description:** ADDENDUM_1: RFP for Managed and Hosted Voice Services

**Proc Type:** Statewide MA (Open End)

| Date Issued | Solicitation Closes | Solicitation No | Version |
|---|---|---|---|
| 2018-10-19 | 2018-11-21<br>13:30:00 | CRFP 0212 SWC1900000001 | 2 |

**BID RECEIVING LOCATION**

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

**VENDOR**

**Vendor Name, Address and Telephone Number:**

Verizon Business Network Services Inc. on behalf of MCI Communications Services, Inc. dba Verizon Business Services
Sandra Hawkins
4700 Maccorkle Avenue
Charleston, WV 25304
Phone: 304-356-3395

**FOR INFORMATION CONTACT THE BUYER**

Mark A Atkins
(304) 558-2307
mark.a.atkins@wv.gov

**Signature X** **FEIN #** 47-0751768 **DATE** November 20, 2018

**All offers subject to all terms and conditions contained in this solicitation**

**ADDITIONAL INFORMATION:**

ADDENDUM_1 Is issued for the following:
1. To move the bid opening date from 10/24/2018 to 11/21/2018/2018 at 1:30pm EST.
2. To publish the mandatory Pre-Bid attendance sheets.
   To permit the agency more time in preparing the responses to the questions submitted by vendors during the Technical Questioning period.

No other changes made.

The West Virginia Department of Administration, Purchasing Division (hereinafter referred to as the "Purchasing Division") is issuing this solicitation as a request for proposal ("RFP"), as authorized by W. Va. Code 5A-3-10b, for the West Virginia Office of Technology (hereinafter referred to as the "Agency") to provide Managed Voice Services for the State's Legacy VoIP Environment, while working to migrate those Legacy Environments to a Hosted VoIP Platform, included Hosted Contact Center Services per attached documents.

MANDATORY PRE-BID MEETING:
DATE: 09/26/2018
TIME: 2:30PM EDT
LOCATION: WV Office of Technology

NOTE: Online responses to this solicitation are prohibited. Please see the Instructions to Bidders in Section 2 for proposal submission.

| INVOICE TO | | SHIP TO | |
|---|---|---|---|
| ALL STATE AGENCIES<br>VARIOUS LOCATIONS AS INDICATED BY ORDER | | STATE OF WEST VIRGINIA<br>VARIOUS LOCATIONS AS INDICATED BY ORDER | |
| No City | WV99999 | No City | WV 99999 |
| US | | US | |

| Line | Comm Ln Desc | Qty | Unit Issue | Unit Price | Total Price |
|---|---|---|---|---|---|
| 1 | Managed and Hosted Voice Services | 0.00000 | EA | | |

| mm Code | Manufacturer | Specification | Model # |
|---|---|---|---|
| 161700 | | | |

**Extended Description :**

See Attachment_A Cost Sheet for proposal pricing.

Vendor shall use the Attachment_A Cost Sheet for proposal pricing.

Note: online proposal submissions are prohibited.

Please see Section 5 Vendor Proposal Subsection 5.3 for further instructions.

**SCHEDULE OF EVENTS**

| Line | Event | Event Date |
|---|---|---|
| 1 | Mandatory Pre-Bid Meeting @ 2:30pm EDT: | 2018-09-26 |
| 2 | Technical Questions due by 2:00pm EDT: | 2018-10-05 |

## ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

Purchasing Divison
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

**State of West Virginia**
**Request for Proposal**
**35 — Telecomm**

**Proc Folder:** 462803

**Doc Description:** ADDENDUM_2: RFP for Managed and Hosted Voice Services

**Proc Type:** Statewide MA (Open End)

| Date Issued | Solicitation Closes | Solicitation No | Version |
|---|---|---|---|
| 2018-10-25 | 2018-11-21<br>13:30:00 | CRFP 0212 SWC1900000001 | 3 |

**BID RECEIVING LOCATION**

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

**VENDOR**

**Vendor Name, Address and Telephone Number:**

Verizon Business Network Services Inc. on behalf of MCI Communications Services, Inc. dba Verizon Business Services
Sandra Hawkins
4700 Maccorkle Avenue
Charleston, WV 25304
Phone: 304-356-3395

**FOR INFORMATION CONTACT THE BUYER**

Mark A Atkins
(304) 558-2307
mark.a.atkins@wv.gov

**ꞁnature X** **FEIN #** 47-0751768 **DATE** November 20, 2018

**All offers subject to all terms and conditions contained in this solicitation**

## ADDITIONAL INFORMATION:

ADDENDUM_2 Is issued for the following:

1. To Publish revised specifications (rev. 10-24-2018).
2. To Publish revised Attachment_A Cost Sheet. (rev. 10-24-2018 Excel formatted).
   To Publish revised Appendix_A document (rev. 10-24-2018).
   'o publish the Agency's response to the questions submitted by Vendors during the Technical Questioning period.
5. To open a second Technical Question period until 11/01/2018 due by 2:00pm EDT.

No other changes made.

The West Virginia Department of Administration, Purchasing Division (hereinafter referred to as the "Purchasing Division") is issuing this solicitation as a request for proposal ("RFP"), as authorized by W. Va. Code 5A-3-10b, for the West Virginia Office of Technology (hereinafter referred to as the "Agency") to provide Managed Voice Services for the State's Legacy VoIP Environment, while working to migrate those Legacy Environments to a Hosted VoIP Platform, included Hosted Contact Center Services per attached documents.

MANDATORY PRE-BID MEETING:
DATE: 09/26/2018
TIME: 2:30PM EDT
LOCATION: WV Office of Technology

NOTE: Online responses to this solicitation are prohibited. Please see the Instructions to Bidders in Section 2 for proposal submission.

| INVOICE TO | | SHIP TO | |
|---|---|---|---|
| ALL STATE AGENCIES<br>VARIOUS LOCATIONS AS INDICATED BY ORDER | | STATE OF WEST VIRGINIA<br>VARIOUS LOCATIONS AS INDICATED BY ORDER | |
| No City | WV99999 | No City | WV 99999 |
| US | | US | |

| Line | Comm Ln Desc | Qty | Unit Issue | Unit Price | Total Price |
|---|---|---|---|---|---|
| 1 | Managed and Hosted Voice Services | 0.00000 | EA | | |

| Comm Code | Manufacturer | Specification | Model # |
|---|---|---|---|
| 81161700 | | | |

**Extended Description :**

See Attachment_A Cost Sheet for proposal pricing.

Vendor shall use the Attachment_A Cost Sheet for proposal pricing.

Note: online proposal submissions are prohibited.

Please see Section 5 Vendor Proposal Subsection 5.3 for further instructions.

## SCHEDULE OF EVENTS

| Line | Event | Event Date |
|---|---|---|
| 1 | Mandatory Pre-Bid Meeting @ 2:30pm EDT: | 2018-09-26 |
| 2 | Technical Questions due by 2:00pm EDT: | 2018-10-05 |
| 3 | Technical Questions due by 2:00pm EDT: | 2018-11-01 |

## ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

Purchasing Divison
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Request for Proposal
35 — Telecomm

Proc Folder: 462803

Doc Description: ADDENDUM_3: RFP for Managed and Hosted Voice Services

Proc Type: Statewide MA (Open End)

| Date Issued | Solicitation Closes | Solicitation No | Version |
|---|---|---|---|
| 2018-11-02 | 2018-11-21<br>13:30:00 | CRFP 0212 SWC1900000001 | 4 |

**BID RECEIVING LOCATION**

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

**VENDOR**

Vendor Name, Address and Telephone Number:

Verizon Business Network Services Inc. on behalf of MCI Communications Services, Inc. dba
Verizon Business Services
Sandra Hawkins
4700 Maccorkle Avenue
Charleston, WV 25304
Phone: 304-356-3395

FOR INFORMATION CONTACT THE BUYER

Mark A Atkins
(304) 558-2307
mark.a.atkins@wv.gov

Signature X FEIN # 47-0751768 DATE November 20, 2018

All offers subject to all terms and conditions contained in this solicitation

**ADDITIONAL INFORMATION:**

ADDENDUM_3 Is issued for the following:
1. To publish the Agency's response to the questions submitted by Vendors during the Technical Questioning second and final period.
2. To Publish revised Attachment_A Cost Sheet. (rev 11-02-2018 Excel formatted).

No other changes made.

The West Virginia Department of Administration, Purchasing Division (hereinafter referred to as the "Purchasing Division") is issuing this solicitation as a request for proposal ("RFP"), as authorized by W. Va. Code 5A-3-10b, for the West Virginia Office of Technology (hereinafter referred to as the "Agency") to provide Managed Voice Services for the State's Legacy VoIP Environment, while working to migrate those Legacy Environments to a Hosted VoIP Platform, included Hosted Contact Center Services per attached documents.

MANDATORY PRE-BID MEETING:
DATE: 09/26/2018
TIME: 2:30PM EDT
LOCATION: WV Office of Technology

NOTE: Online responses to this solicitation are prohibited. Please see the Instructions to Bidders in Section 2 for proposal submission.

| INVOICE TO | SHIP TO |
|---|---|
| ALL STATE AGENCIES<br>VARIOUS LOCATIONS AS INDICATED BY ORDER | STATE OF WEST VIRGINIA<br>VARIOUS LOCATIONS AS INDICATED BY ORDER |
| No City WV99999 | No City WV 99999 |
| US | US |

| Line | Comm Ln Desc | Qty | Unit Issue | Unit Price | Total Price |
|---|---|---|---|---|---|
| 1 | Managed and Hosted Voice Services | 0.00000 | EA | | |

| Comm Code | Manufacturer | Specification | Model # |
|---|---|---|---|
| 81161700 | | | |

**Extended Description :**

See Attachment_A Cost Sheet for proposal pricing. (Revised 11-02-2018)

Vendor shall use the Attachment_A Cost Sheet for proposal pricing.

Note: online proposal submissions are prohibited.

Please see Section 5 Vendor Proposal Subsection 5.3 for further instructions.

**SCHEDULE OF EVENTS**

| Line | Event | Event Date |
|---|---|---|
| 1 | Mandatory Pre-Bid Meeting @ 2:30pm EDT: | 2018-09-26 |
| 2 | Technical Questions due by 2:00pm EDT: | 2018-10-05 |
| 3 | Technical Questions due by 2:00pm EDT: | 2018-11-01 |

# SOLICITATION NUMBER: CRFP 0212 SWC1900000001
# Addendum Number: 3

The purpose of this addendum is to modify the solicitation identified as CRFP 0212 SWC1900000001 ("Solicitation") to reflect the change(s) identified and described below.

**Applicable Addendum Category:**

[ ] Modify bid opening date and time

[ ] Modify specifications of product or service being sought

[X] Attachment of vendor questions and responses for round #2 (final round of questions permitted)

[ ] Attachment of pre-bid sign-in sheet

[ ] Correction of error

[X] Publish revised Cost Sheets

**Description of Modification to Solicitation:**

1. **To publish the Agency's response to the questions submitted by Vendors during the Technical Questioning second and final period.**
2. **To publish the Attachment_A Cost Sheets (Revised 11-02-2018)**

No other changes made.

**Additional Documentation:** Documentation related to this Addendum (if any) has been included herewith as Attachment A and is specifically incorporated herein by reference.

**Terms and Conditions:**

1. All provisions of the Solicitation and other addenda not modified herein shall remain in full force and effect.

2. Vendor should acknowledge receipt of all addenda issued for this Solicitation by completing an Addendum Acknowledgment, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

Purchasing Divison
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

**State of West Virginia**
**Request for Proposal**
**35 — Telecomm**

**Proc Folder:** 462803

**Doc Description:** ADDENDUM_4: RFP for Managed and Hosted Voice Services

**Proc Type:** Statewide MA (Open End)

| Date Issued | Solicitation Closes | Solicitation No | Version |
|---|---|---|---|
| 2018-11-15 | 2018-11-21<br>13:30:00 | CRFP 0212 SWC1900000001 | 5 |

**BID RECEIVING LOCATION**

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

**VENDOR**

**Vendor Name, Address and Telephone Number:**

Verizon Business Network Services Inc. on behalf of MCI Communications Services, Inc. dba
Verizon Business Services
Sandra Hawkins
4700 Maccorkle Avenue
Charleston, WV 25304
Phone: 304-356-3395

**FOR INFORMATION CONTACT THE BUYER**

Mark A Atkins
(304) 558-2307
mark.a.atkins@wv.gov

**nature X** **FEIN #** 47-0751768 **DATE** November 20, 2018

**All offers subject to all terms and conditions contained in this solicitation**

**ADDITIONAL INFORMATION:**

ADDENDUM_4 Is issued for the following:
1. To Publish revised Attachment_A Cost Sheet. (rev. 11-15-2018 Excel formatted) due to a calculation error.

› other changes made.

ı ne West Virginia Department of Administration, Purchasing Division (hereinafter referred to as the "Purchasing Division") is issuing this solicitation as a request for proposal ("RFP"), as authorized by W. Va. Code 5A-3-10b, for the West Virginia Office of Technology (hereinafter referred to as the "Agency") to provide Managed Voice Services for the State's Legacy VoIP Environment, while working to migrate those Legacy Environments to a Hosted VoIP Platform, included Hosted Contact Center Services per attached documents.

MANDATORY PRE-BID MEETING:
DATE: 09/26/2018
TIME: 2:30PM EDT
LOCATION: WV Office of Technology

NOTE: Online responses to this solicitation are prohibited. Please see the Instructions to Bidders in Section 2 for proposal submission.

| INVOICE TO | SHIP TO |
|---|---|
| ALL STATE AGENCIES<br>VARIOUS LOCATIONS AS INDICATED BY ORDER<br>No City WV99999<br>US | STATE OF WEST VIRGINIA<br>VARIOUS LOCATIONS AS INDICATED BY ORDER<br>No City WV 99999<br>US |

| Line | Comm Ln Desc | Qty | Unit Issue | Unit Price | Total Price |
|---|---|---|---|---|---|
| 1 | Managed and Hosted Voice Services | 0.00000 | EA | | |

| Comm Code | Manufacturer | Specification | Model # |
|---|---|---|---|
| ²1161700 | | | |

**Extended Description :**

See Attachment_A Cost Sheet for proposal pricing. (Revised 11-02-2018)

Vendor shall use the Attachment_A Cost Sheet for proposal pricing.

Note: online proposal submissions are prohibited.

Please see Section 5 Vendor Proposal Subsection 5.3 for further instructions.

**SCHEDULE OF EVENTS**

| Line | Event | Event Date |
|---|---|---|
| 1 | Mandatory Pre-Bid Meeting @ 2:30pm EDT: | 2018-09-26 |
| 2 | Technical Questions due by 2:00pm EDT: | 2018-10-05 |
| 3 | Technical Questions due by 2:00pm EDT: | 2018-11-01 |

## ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

Purchasing Divison
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

**State of West Virginia**
**Request for Proposal**
**35 — Telecomm**

**Proc Folder:** 462803

**Doc Description:** ADDENDUM_5: RFP for Managed and Hosted Voice Services

**Proc Type:** Statewide MA (Open End)

| Date Issued | Solicitation Closes | Solicitation No | Version |
|---|---|---|---|
| 2018-11-16 | 2018-11-27<br>13:30:00 | CRFP 0212 SWC1900000001 | 6 |

**BID RECEIVING LOCATION**

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

**VENDOR**

**Vendor Name, Address and Telephone Number:**

Verizon Business Network Services Inc. on behalf of MCI Communications Services, Inc. dba
Verizon Business Services
Sandra Hawkins
4700 Maccorkle Avenue
Charleston, WV 25304
Phone: 304-356-3395

**FOR INFORMATION CONTACT THE BUYER**

Mark A Atkins
(304) 558-2307
mark.a.atkins@wv.gov

**gnature X** **FEIN #** 47-0751768 **DATE** November 20, 2018

**All offers subject to all terms and conditions contained in this solicitation**

## ADDITIONAL INFORMATION:

ADDENDUM_5 Is issued for the following:
1. To move the Bid Opening date from 11/21/2018 to 11/27/2018 at 1:30pm EST.
2. To Publish revised Attachment_A Cost Sheet. (rev. 11-16-2018 Excel formatted) due to a calculation error.

other changes made.

The West Virginia Department of Administration, Purchasing Division (hereinafter referred to as the "Purchasing Division") is issuing this solicitation as a request for proposal ("RFP"), as authorized by W. Va. Code 5A-3-10b, for the West Virginia Office of Technology (hereinafter referred to as the "Agency") to provide Managed Voice Services for the State's Legacy VoIP Environment, while working to migrate those Legacy Environments to a Hosted VoIP Platform, included Hosted Contact Center Services per attached documents.

MANDATORY PRE-BID MEETING:
DATE: 09/26/2018
TIME: 2:30PM EDT
LOCATION: WV Office of Technology

NOTE: Online responses to this solicitation are prohibited. Please see the Instructions to Bidders in Section 2 for proposal submission.

| INVOICE TO | | SHIP TO | |
|---|---|---|---|
| ALL STATE AGENCIES<br>VARIOUS LOCATIONS AS INDICATED BY ORDER | | STATE OF WEST VIRGINIA<br>VARIOUS LOCATIONS AS INDICATED BY ORDER | |
| No City | WV99999 | No City | WV 99999 |
| US | | US | |

| Line | Comm Ln Desc | Qty | Unit Issue | Unit Price | Total Price |
|---|---|---|---|---|---|
| 1 | Managed and Hosted Voice Services | 0.00000 | EA | | |

| Comm Code | Manufacturer | Specification | Model # |
|---|---|---|---|
| 161700 | | | |

**Extended Description :**

See Attachment_A Cost Sheet for proposal pricing. (Revised 11-16-2018)

Vendor shall use the Attachment_A Cost Sheet for proposal pricing.

Note: online proposal submissions are prohibited.

Please see Section 5 Vendor Proposal Subsection 5.3 for further instructions.

## SCHEDULE OF EVENTS

| Line | Event | Event Date |
|---|---|---|
| 1 | Mandatory Pre-Bid Meeting @ 2:30pm EDT: | 2018-09-26 |
| 2 | Technical Questions due by 2:00pm EDT: | 2018-10-05 |
| 3 | Technical Questions due by 2:00pm EDT: | 2018-11-01 |

## ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

# *Section 1: General Information*

## *1.1. Introduction*

### Verizon Response

Verizon has read and understands.

## *1.2. RFP Schedule of Events*

- *RFP Released to Public 08/29/2018*
- *Mandatory Pre-bid Conference 09/26/2018 @ 2:30 pm EDT*
- *Vendor's Written Questions Submission Deadline 10/05/2018 by 2:00 pm EDT*
- *Addendum Issued TBD*
- *Technical Bid Opening Date 10/24/2018 at 1:30 pm EDT*
- *Technical Evaluation Begins 10/24/2018*
- *Oral Presentation TBD*
- *Cost Bid Opening TBD*
- *Cost Evaluation Begins TBD*
- *Contract Award Made TBD*

### Verizon Response

Verizon has read, understands, and will comply with Addendum 5, "Technical Bid Opening Date Change" of 11/27/18, at 1:30 pm.

# Section 2. Instructions to Vendors Submitting Bids

## *Instructions to Vendors Submitting Bids*

### *1. Review Documents Thoroughly*

*The attached documents contain a solicitation for bids. Please read these instructions and all documents attached in their entirety. These instructions provide critical information about requirements that if overlooked could lead to disqualification of a Vendor's bid.*

*All bids must be submitted in accordance with the provisions contained in these instructions and the Solicitation. Failure to do so may result in disqualification of Vendor's bid.*

**Verizon Response**

Verizon has read and understands.

### *2. Mandatory Terms*

*The Solicitation may contain mandatory provisions identified by the use of the words "must," "will," and "shall."Failure to comply with a mandatory term in the Solicitation will result in bid disqualification.*

**Verizon Response**

Verizon has read and understands.

### *3. Prebid Meeting*

*The item identified below shall apply to this Solicitation.*

*__ A pre-bid meeting will not be held prior to bid opening*

*__ A NON-MANDATORY PRE-BID meeting will be held at the following place and time*

*X A MANDATORY PRE-BID meeting will be held at the following place and time*

*DATE: 09/26/2018 TIME: 2:30pm EDT*

*LOCATION: West Virginia Office of Technology, 1900 Kanawha Blvd. E., Building 5, 10th Floor Charleston, WV 25305*

*All Vendors submitting a bid must attend the mandatory pre-bid meeting. Failure to attend the mandatory pre-bid meeting shall result in disqualification of the Vendor's bid. No one person attending the pre-bid meeting may represent more than one Vendor.*

*An attendance sheet provided at the pre-bid meeting shall serve as the official document verifying attendance. The State will not accept any other form of proof or documentation to verify attendance. Any person attending the pre-bid meeting on behalf of a Vendor must list on the attendance sheet his or her name and the name of the Vendor he or she is representing.*

*Additionally, the person attending the pre-bid meeting should include the Vendor's E-Mail address, phone number, and Fax number on the attendance sheet. It is the Vendor's responsibility to locate the attendance sheet and provide the required information. Failure to complete the attendance sheet as required may result in disqualification of Vendor's bid.*

*All Vendors should arrive prior to the starting time for the pre-bid. Vendors who arrive after the starting time but prior to the end of the pre-bid will be permitted to sign in, but are charged with knowing all matters discussed at the pre-bid.*

*Questions submitted at least five business days prior to a scheduled pre-bid will be discussed at the pre-bid meeting if possible. Any discussions or answers to questions at the pre-bid meeting are preliminary in nature and are non-binding. Official and binding answers to questions will be published in a written addendum to the Solicitation prior to bid opening.*

**Verizon Response**

Verizon has read and understands.

### 4. Vendor Question Deadline

*Vendors may submit questions relating to this Solicitation to the Purchasing Division. Questions must be submitted in writing. All questions must be submitted on or before the date listed below and to the address listed below in order to be considered.*

*A written response will be published in a Solicitation addendum if a response is possible and appropriate. Non-written discussions, conversations, or questions and answers regarding this Solicitation are preliminary in nature and are nonbinding.*

*Submitted e-mails should have solicitation number in the subject line. Question Submission Deadline: October 05, 2018 due by 2:00pm EDT*

*Submit Questions to:*

*Mark Atkins, Senior Buyer*
*2019 Washington Street,*
*East Charleston, WV 25305*
*Fax: (304) 558-4115 (Vendors should not use this fax number for bid submission)*
*Email: Mark.A.Atkins@wv.gov*

**Verizon Response**

Verizon has read and understands.

### 5. Verbal Communication

*Any verbal communication between the Vendor and any State personnel is not binding, including verbal communication at the mandatory pre-bid conference. Only information issued in writing and added to the Solicitation by an official written addendum by the Purchasing Division is binding.*

**Verizon Response**

Verizon has read and understands.

## 6. Bid Submission

*All bids must be submitted electronically through wvOASIS or signed and delivered by the Vendor to the Purchasing Division at the address listed below on or before the date and time of the bid opening. Any bid received by the Purchasing Division staff is considered to be in the possession of the Purchasing Division and will not be returned for any reason.*

*The Purchasing Division will not accept bids, modification of bids, or addendum acknowledgment forms via e-mail. Acceptable delivery methods include electronic submission via wvOASIS, hand delivery, delivery by courier, or facsimile.*

*The bid delivery address is*

*Department of Administration, Purchasing Division*
*2019 Washington Street East*
*Charleston, WV 25305-0130*

*A bid that is not submitted electronically through wvOASIS should contain the information listed below on the face of the envelope or the bid may be rejected by the Purchasing Division.*

*SEALED BID: VOiP Hosted Services*
*BUYER: Mark Atkins*
*SOLICITATION NO.: CRFP 0212 SWC1900000001*
*BID OPENING DATE: 10/24/2018*
*BID OPENING TIME: 1:30pm EDT*
*FAX NUMBER: 304-558-3970*

*The Purchasing Division may prohibit the submission of bids electronically through wvOASIS at its sole discretion. Such a prohibition will be contained and communicated in the wvOASIS system resulting in the Vendor's inability to submit bids through wvOASIS. Submission of a response to an Expression or Interest or Request for Proposal is not permitted in wvOASIS.*

*For Request For Proposal ("RFP") Responses Only: In the event that Vendor is responding to a request for proposal, the Vendor shall submit one original technical and one original cost proposal plus Five (5) convenience copies of each to the Purchasing Division at the address shown above.*

*Additionally, the Vendor should identify the bid type as either a technical or cost proposal on the face of each bid envelope submitted in response to a request for proposal as follows*

*BID TYPE: (This only applies to CRFP)*

*X Technical*

*X Cost*

### Verizon Response

Verizon has read, understands, and will comply with Addendum 5, "Technical Bid Opening Date Change" of 11/27/18, at 1:30 pm.

## *7. Bid Opening*

*Bids submitted in response to this Solicitation will be opened at the location identified below on the date and time listed below. Delivery of a bid after the bid opening date and time will result in bid disqualification.*

*For purposes of this Solicitation, a bid is considered delivered when confirmation of delivery is provided by wvOASIS (in the case of electronic submission) or when the bid is time stamped by the official Purchasing Division time clock (in the case of hand delivery).*

- *Bid Opening Date and Time: October 24, 2018 at 1:30 pm EDT*
- *Bid Opening Location: Department of Administration, Purchasing Division 2019 Washington Street East, Charleston, WV 25305-0130*

### Verizon Response

Verizon has read, understands, and will comply with Addendum 5, "Technical Bid Opening Date Change" of 11/27/18, at1:30 pm.

## *8. Addendum Acknowledgement*

*Changes or revisions to this Solicitation will be made by an official written addendum issued by the Purchasing Division. Vendor should acknowledge receipt of all addenda issued with this Solicitation by completing an Addendum Acknowledgment Form, a copy of which is included herewith.*

*Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.*

### Verizon Response

Verizon has read and understands.

## *9. Bid Formatting*

*Vendor should type or electronically enter the information onto its bid to prevent errors in the evaluation. Failure to type or electronically enter the information may result in bid disqualification.*

### Verizon Response

Verizon has read and understands.

## *10. Alternate Model or Brand*

*Unless the box below is checked, any model, brand, or specification listed in this Solicitation establishes the acceptable level of quality only and is not intended to reflect a preference for, or in any way favor, a particular brand or vendor.*

*Vendors may bid alternates to a listed model or brand provided that the alternate is at least equal to the model or brand and complies with the required specifications. The equality of any alternate being bid shall be determined by the State at its sole discretion.*

*Any Vendor bidding an alternate model or brand should clearly identify the alternate items in its bid and should include manufacturer's specifications, industry literature, and/or any other relevant documentation demonstrating the equality of the alternate items.*

*Failure to provide information for alternate items may be grounds for rejection of a Vendor's bid.*

*__ This Solicitation is based upon a standardized commodity established under W. Va. Code § 5A-3-61. Vendors are expected to bid the standardized commodity identified. Failure to bid the standardized commodity will result in your firm's bid being rejected.*

**Verizon Response**

Verizon has read and understands.

### 11. Exceptions and Clarifications

*The Solicitation contains the specifications that shall form the basis of a contractual agreement. Vendor shall clearly mark any exceptions, clarifications, or other proposed modifications in its bid. Exceptions to, clarifications of, or modifications of a requirement or term and condition of the Solicitation may result in bid disqualification.*

**Verizon Response**

Verizon has read and understands.

### 12. Communication Limitations

*In accordance with West Virginia Code of State Rules §148-1-6.6, communication with the State of West Virginia or any of its employees regarding this Solicitation during the solicitation, bid, evaluation or award periods, except through the Purchasing Division, is strictly prohibited without prior Purchasing Division approval. Purchasing Division approval for such communication is implied for all agency delegated and exempt purchases.*

**Verizon Response**

Verizon has read and understands.

### 13. Registration

*Prior to Contract award, the apparent successful Vendor must be properly registered with the West Virginia Purchasing Division and must have paid the $125 fee, if applicable.*

**Verizon Response**

Verizon has read, understands, and will comply.

### 14. Unit Price

*Unit prices shall prevail in cases of a discrepancy in the Vendor's bid.*

**Verizon Response**

Verizon has read and understands.

## *15. Preference*

*Vendor Preference may be requested in purchases of motor vehicles or construction and maintenance equipment and machinery used in highway and other infrastructure projects.*

*Any request for preference must be submitted in writing with the bid, must specifically identify the preference requested with reference to the applicable subsection of West Virginia Code § 5A-3-37, and should include with the bid any information necessary to evaluate and confirm the applicability of the requested preference.*

*A request form to help facilitate the request can be found at http://www.state.wv.us/admin/purchase/vrcNen pref.pdf.*

### Verizon Response

Verizon has read and understands.

## *15A. Reciprocal Preference*

*The State of West Virginia applies a reciprocal preference to all solicitations for commodities and printing in accordance with W. Va. Code § 5A-3-37(b). In effect, non-resident vendors receiving a preference in their home states, will see that same preference granted to West Virginia resident vendors bidding against them in West Virginia.*

*A request form to help facilitate the request can be found at http://www.state.wv.us/admin/purchase/vrc/Venpref.pdf.*

### Verizon Response

Verizon has read and understands.

## *16. Small, Women-Owned, or Minority-Owned Businesses*

*For any solicitations publicly advertised for bid, in accordance with West Virginia Code §5A-3- 37(a)(7) and W. Va. CSR § 148-22-9, any non-resident vendor certified as a small, women- owned, or minority-owned business under W. Va. CSR § 148-22-9 shall be provided the same preference made available to any resident vendor.*

*Any non-resident small, women-owned, or minority-owned business must identify itself as such in writing, must submit that writing to the Purchasing Division with its bid, and must be properly certified under W. Va. CSR § 148-22-9 prior to contract award to receive the preferences made available to resident vendors.*

*Preference for a non-resident small, women-owned, or minority owned business shall be applied in accordance with W. Va. CSR § 148-22-9.*

### Verizon Response

Verizon has read and understands.

## 17. Waiver of Minor Irregularities

*The Director reserves the right to waive minor irregularities in bids or specifications in accordance with West Virginia Code of State Rules § 148-1-4.6.*

### Verizon Response

Verizon has read and understands.

## 18. Electronic File Access Restrictions

*Vendor must ensure that its submission in wvOASIS can be accessed and viewed by the Purchasing Division staff immediately upon bid opening.*

*The Purchasing Division will consider any file that cannot be immediately accessed and viewed at the time of the bid opening (such as, encrypted files, password protected files, or incompatible files) to be blank or incomplete as context requires, and are therefore unacceptable.*

*A vendor will not be permitted to unencrypt files, remove password protections, or resubmit documents after bid opening to make a file viewable if those documents are required with the bid.*

*A Vendor may be required to provide document passwords or remove access restrictions to allow the Purchasing Division to print or electronically save documents provided that those documents are viewable by the Purchasing Division prior to obtaining the password or removing the access restriction.*

### Verizon Response

Verizon has read and understands.

## 19. Non-Responsible

*The Purchasing Division Director reserves the right to reject the bid of any vendor as Non-Responsible in accordance with W. Va. Code of State Rules § 148-1- 5.3, when the Director determines that the vendor submitting the bid does not have the capability to fully perform, or lacks the integrity and reliability to assure good-faith performance."*

### Verizon Response

Verizon has read and understands.

## 20. Acceptance/Rejection

*The State may accept or reject any bid in whole, or in part in accordance with W. Va. Code of State Rules § 148-1-4.5. and § 148-1-6.4.b."*

### Verizon Response

Verizon has read and understands.

## *21. Your Submission Is a Public Document*

*Vendor's entire response to the Solicitation and the resulting Contract are public documents.*

*As public documents, they will be disclosed to the public following the bid/proposal opening or award of the contract, as required by the competitive bidding laws of West Virginia Code §§ 5A-3-1 et seq., 5-22-1 et seq., and 5G-1-1 et seq. and the Freedom ofInformation Act West Virginia Code §§ 29B-1-1 et seq.*

*DO NOT SUBMIT MATERIAL YOU CONSIDER TO BE CONFIDENTIAL, A TRADE SECRET, OR OTHERWISE NOT SUBJECT TO PUBLIC DISCLOSURE.*

*Submission of any bid, proposal, or other document to the Purchasing Division constitutes your explicit consent to the subsequent public disclosure of the bid, proposal, or document.*

*The Purchasing Division will disclose any document labeled "confidential," "proprietary," "trade secret," "private," or labeled with any other claim against public disclosure of the documents, to include any "trade secrets" as defined by West Virginia Code § 47-22-1 et seq. All submissions are subject to public disclosure without notice.*

### Verizon Response

Verizon has read and understands.

## *22. Interested Party Disclosure*

*West Virginia Code § 6D-I -2 requires that the vendor submit to the Purchasing Division a disclosure of interested parties to the contract for all contracts with an actual or estimated value of at least $1 Million.*

*That disclosure must occur on the form prescribed and approved by the WV Ethics Commission prior to contract award. A copy of that form is included with this solicitation or can be obtained from the WV Ethics*

*Commission. This requirement does not apply to publicly traded companies listed on a national or international stock exchange. A more detailed definition of interested parties can be obtained from the form referenced above.*

### Verizon Response

Verizon has read and understands.

## *23. With the Bid Requirements*

*In instances where these specifications require documentation or other information with the bid, and a vendor fails to provide it with the bid, the Director of the Purchasing Division reserves the right to request those items after bid opening and prior to contract award pursuant to the authority to waive minor irregularities in bids or specifications under W. Va. CSR § 148-1-4.6.*

*This authority does not apply to instances where state law mandates receipt with the bid.*

### Verizon Response

Verizon has read and understands.

# Section 3. General Terms and Conditions

## *General Terms and Conditions*

### *1. Contractual Agreement*

*Issuance of a Award Document signed by the Purchasing Division Director, or his designee, and approved as to form by the Attorney General's office constitutes acceptance of this Contract made by and between the State of West Virginia and the Vendor.*

*Vendor's signature on its bid signifies Vendor's agreement to be bound by and accept the terms and conditions contained in this Contract.*

**Verizon Response**

Notwithstanding anything to the contrary contained in the RFP documents, Verizon does not consider this RFP response as legally binding to provide the Services described herein until all exceptions have been resolved, a mutual understanding is reached, and a contract is executed.

### *2. Definitions*

*As used in this Solicitation/Contract, the following terms shall have the meanings attributed to them below. Additional definitions may be found in the specifications included with this Solicitation/Contract.*

*2.1. "Agency" or "Agencies" means the agency, board, commission, or other entity of the State of West Virginia that is identified on the first page of the Solicitation or any other public entity seeking to procure goods or services under this Contract.*

*2.2. "Bid" or "Proposal" means the vendors submitted response to this solicitation.*

*2.3. "Contract" means the binding agreement that is entered into between the State and the Vendor to provide the goods or services requested in the Solicitation.*

*2.4. "Director" means the Director of the West Virginia Department of Administration, Purchasing Division.*

*2.5. "Purchasing Division" means the West Virginia Department of Administration, Purchasing Division.*

*2.6. "Award Document" means the document signed by the Agency and the Purchasing Division, and approved as to form by the Attorney General, that identifies the Vendor as the contract holder.*

*2.7. "Solicitation" means the official notice of an opportunity to supply the State with goods or services that is published by the Purchasing Division.*

*2.8. "State" means the State of West Virginia and/or any of its agencies, commissions, boards, etc. as context requires.*

*2.9. "Vendor" or "Vendors" means any entity submitting a bid in response to the Solicitation, the entity that has been selected as the lowest responsible bidder, or the entity that has been awarded the Contract as context requires.*

**Verizon Response**

Verizon has read and understands.

### *3. Contract Term; Renewal; Extension*

*The term of this Contract shall be determined in accordance with the category that has been identified as applicable to this Contract below*

*X Term Contract*

*Initial Contract Term: Initial Contract Term: This Contract becomes effective on Upon award and extends for a period of Four (4) year(s).*

*Renewal Term: This Contract may be renewed upon the mutual written consent of the Agency, and the Vendor, with approval of the Purchasing Division and the Attorney General's office (Attorney General approval is as to form only).*

*Any request for renewal should be delivered to the Agency and then submitted to the Purchasing Division thirty (30) days prior to the expiration date of the initial contract term or appropriate renewal term. A Contract renewal shall be in accordance with the terms and conditions of the original contract.*

*Unless otherwise specified below, renewal of this Contract is limited to see below successive one (I ) year periods or multiple renewal periods of less than one year, provided that the multiple renewal periods do not exceed the total number of months available in all renewal years combined.*

*Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General 's office (Attorney General approval is as to form only)*

*X Alternate Renewal Term - This contract may be renewed for Two (2) successive Two (2) year periods or shorter periods provided that they do not exceed the total number of months contained in all available renewals. Automatic renewal of this Contract is prohibited.*

*Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's office (Attorney General approval is as to form only)*

*__ Delivery Order Limitations: In the event that this contract permits delivery orders, a delivery order may only be issued during the time this Contract is in effect. Any delivery order issued within one year of the expiration of this Contract shall be effective for one year from the date the delivery order is issued. No delivery order may be extended beyond one year after this Contract has expired.*

*__ Fixed Period Contract: This Contract becomes effective upon Vendor's receipt of the notice to proceed and must be completed within ___ days.*

*__ Fixed Period Contract with Renewals: This Contract becomes effective upon Vendor's receipt of the notice to proceed and part of the Contract more fully described in the attached specifications must be completed within ____ days. Upon completion of the work covered by the preceding sentence, the vendor agrees that maintenance, monitoring, or warranty services will be provided for ___ year(s) thereafter.*

*__ One Time Purchase: The term of this Contract shall run from the issuance of the Award Document until all of the goods contracted for have been delivered, but in no event will this Contract extend for more than one fiscal year.*

*__ Other: See attached.*

**Verizon Response**

Verizon has read and understands.

## 4. Notice to Proceed

*Vendor shall begin performance of this Contract immediately upon receiving notice to proceed unless otherwise instructed by the Agency. Unless otherwise specified, the fully executed Award Document will be considered notice to proceed.*

### Verizon Response

Verizon has read and understands.

## 5. Quantities

*The quantities required under this Contract shall be determined in accordance with the category that has been identified as applicable to this Contract below.*

*X Open End Contract: Quantities listed in this Solicitation are approximations only, based on estimates supplied by the Agency. It is understood and agreed that the Contract shall cover the quantities actually ordered for delivery during the term of the Contract, whether more or less than the quantities shown.*

*X Service: The scope of the service to be provided will be more clearly defined in the specifications included herewith.*

*__ Combined Service and Goods: The scope of the service and deliverable goods to be provided will be more clearly defined in the specifications included herewith.*

*__ One Time Purchase: This Contract is for the purchase of a set quantity of goods that are identified in the specifications included herewith. Once those items have been delivered, no additional goods may be procured under this Contract without an appropriate change order approved by the Vendor, Agency, Purchasing Division, and Attorney General 's office.*

### Verizon Response

Verizon has read and understands.

## 6. Emergency Purchases

*The Purchasing Division Director may authorize the Agency to purchase goods or services in the open market that Vendor would otherwise provide under this Contract if those goods or services are for immediate or expedited delivery in an emergency.*

*Emergencies shall include, but are not limited to, delays in transportation or an unanticipated increase in the volume of work.*

*An emergency purchase in the open market, approved by the Purchasing Division Director, shall not constitute of breach of this Contract and shall not entitle the Vendor to any form of compensation or damages. This provision does not excuse the State from fulfilling its obligations under a One Time Purchase contract.*

### Verizon Response

Verizon has read and understands.

## 7. Required Documents

*All of the items checked below must be provided to the Purchasing Division by the Vendor as specified below.*

*__ BID BOND (Construction Only): Pursuant to the requirements contained in W. Va. Code § 5-22-1(c), All Vendors submitting a bid on a construction project shall furnish a valid bid bond in the amount of five percent (5%) of the total amount of the bid protecting the State of West Virginia. The bid bond must be submitted with the bid.*

*__ PERFORMANCE BOND: The apparent successful Vendor shall provide a performance bond in the amount of 100% of the contract. The performance bond must be received by the Purchasing Division prior to Contract award.*

*__ LABOR/MATERIAL PAYMENT BOND: The apparent successful Vendor shall provide a labor/material payment bond in the amount of 100% of the Contract value. The labor/material payment bond must be delivered to the Purchasing Division prior to Contract award.*

*In lieu of the Bid Bond, Performance Bond, and Labor/Material Payment Bond, the Vendor may provide certified checks, cashier's checks, or irrevocable letters of credit. Any certified check, cashier's check, or irrevocable letter of credit provided in lieu of a bond must be of the same amount and delivered on the same schedule as the bond it replaces.*

*A letter of credit submitted in lieu of a performance and labor/material payment bond will only be allowed for projects under $100,000. Personal or business checks are not acceptable.*

*Notwithstanding the foregoing, West Virginia Code § 5-22-1 (d) mandates that a vendor provide a performance and labor/material payment bond for construction projects. Accordingly, substitutions for the performance and labor/material payment bonds for construction projects is not permitted.*

*__ MAINTENANCE BOND: The apparent successful Vendor shall provide a two (2) year maintenance bond covering the roofing system. The maintenance bond must be issued and delivered to the Purchasing Division prior to Contract award.*

*__ LICENSE(S) I CERTIFICATIONS I PERMITS: In addition to anything required under the Section of the General Terms and Conditions entitled Licensing, the apparent successful Vendor shall furnish proof of the following licenses, certifications, and/or permits prior to Contract award, in a form acceptable to the Purchasing Division.*

*The apparent successful Vendor shall also furnish proof of any additional licenses or certifications contained in the specifications prior to Contract award regardless of whether or not that requirement is listed above.*

### Verizon Response

Verizon has read and understands.

## 8. Insurance

*The apparent successful Vendor shall furnish proof of the insurance identified by a checkmark below and must include the State as an additional insured on each policy prior to Contract award. The insurance coverages identified below must be maintained throughout the life of this contract.*

*Thirty (30) days prior to the expiration of the insurance policies, Vendor shall provide the Agency with proof that the insurance mandated herein has been continued.*

*Vendor must also provide Agency with immediate notice of any changes in its insurance policies, including but not limited to, policy cancelation, policy reduction, or change in insurers.*

*The apparent successful Vendor shall also furnish proof of any additional insurance requirements contained in the specifications prior to Contract award regardless of whether or not that*

*insurance requirement is listed in this section.*

*Vendor must maintain*

*X Commercial General Liability Insurance in at least an amount of: $ 1,000,000.00 per occurrence.*

*X Automobile Liability Insu rance in at least an amount of: $1,000,000.00 per occurrence.*

*__ Professional/Malpractice/Errors and Omission Insurance in at least an amount of: ____ per occurrence.*

*__ Commercial Crime and Third Party Fidelity Insurance in an amount of: __ per occurrence.*

*X Cyber Liability Insurance in an amount of: $3,000,000 per occurrence.*

*__Builders Risk Insurance in an amount equal to 100% of the amount of the Contract.*

*__ Pollution Insu rance in an amount of: per occurrence.*

*__ Aircraft Liability in an amount of: per occurrence.*

*Notwithstanding anything contained in this section to the contrary, the Director of the Purchasing Division reserves the right to waive the requirement that the State be named as an additional insured on one or more of the Vendor's insurance policies if the Director finds that doing so is in the State's best interest.*

## Verizon Response

Verizon would like to propose the following language:

"The apparent successful Vendor shall furnish proof of the insurance identified by a checkmark below and must include the State as an additional insured as their interest may appear under this Agreement on the commercial general liability and commercial automobile liability ~~on each~~ polic~~y~~ies upon ~~prior to~~ Contract award. The insurance coverages identified below must be maintained throughout the life of this contract.

Within Thirty (30) days of ~~prior to~~ the expiration of the insurance policies, Vendor shall provide the Agency with proof that the insurance mandated herein has been continued.

Upon receipt of notice from its insurer(s) Vendor will ~~must also~~ provide Agency with thirty (30) days prior written notice of cancellation of any coverage required herein. ~~immediate notice of any changes in its insurance policies, including but not limited to, policy cancelation, policy reduction, or change in insurers.~~

~~The apparent successful Vendor shall also furnish proof of any additional insurance requirements contained in the specifications prior to Contract award regardless of whether or not that insurance requirement is listed in this section.~~

Vendor must maintain

X Commercial General Liability Insurance in ~~at least~~ an amount of: $ 1,000,000.00 per occurrence for bodily injury and property damage.

X Automobile Liability Insurance in ~~at least~~ an amount of: $1,000,000.00 combined single limit each accident ~~per occurrence~~.

__ Professional/Malpractice/Errors and Omission Insurance in at least an amount of per occurrence.

__ Commercial Crime and Third Party Fidelity Insurance in an amount of: __ per occurrence.

X Telecommunications, Media & Technology Errors and Omissions including Cyber Liability Insurance in an amount of: $3,000,000 per claim and aggregate ~~occurrence~~.

__Builders Risk Insurance in an amount equal to 100% of the amount of the Contract.

__ Pollution Insurance in an amount of: per occurrence.

__Aircraft Liability in an amount of: per occurrence.

Notwithstanding anything contained in this section to the contrary, the Director of the Purchasing Division reserves the right to waive the requirement that the State be named as an additional insured on one or more of the Vendor's insurance policies if the Director finds that doing so is in the State's best interest."

For additional information, please reference our evidence of liability coverage provided in Appendix F of this proposal. Actual certificates will be issued on award.

## *9. Workers' Compensation Insurance*

*The apparent successful Vendor shall comply with laws relating to workers compensation, shall maintain workers' compensation insurance when required, and shall furnish proof of workers' compensation insurance upon request.*

### Verizon Response

Verizon has read and understands.

### *10. [Reserved]*

### *11. Liquidated Damages*

*This clause shall in no way be considered exclusive and shall not limit the State or Agency's right to pursue any other available remedy. Vendor shall pay liquidated damages in the amount specified below or as described in the specifications:*

_______ *for* _________

___ *Liquidated Damages Contained in the Specifications*

**Verizon Response**

Verizon has read and understands.

### *12. Acceptance*

*Vendor's signature on its bid, or on the certification and signature page, constitutes an offer to the State that cannot be unilaterally withdrawn, signifies that the product or service proposed by vendor meets the mandatory requirements contained in the Solicitation for that product or service, unless otherwise indicated, and signifies acceptance of the terms and conditions contained in the Solicitation unless otherwise indicated.*

**Verizon Response**

Notwithstanding anything to the contrary contained in the RFP documents, Verizon does not consider this RFP response as legally binding to provide the Services described herein until all exceptions have been resolved, a mutual understanding is reached, and a contract is executed.

### *13. Pricing*

*The pricing set forth herein is firm for the life of the Contract, unless specified elsewhere within this Solicitation/Contract by the State. A Vendor's inclusion of price adjustment provisions in its bid, without an express authorization from the State in the Solicitation to do so, may result in bid disqualification.*

**Verizon Response**

Verizon has read and understands.

### *14. Payment in Arrears*

*Payment in advance is prohibited under this Contract. Payment may only be made after the delivery and acceptance of goods or services. The Vendor shall submit invoices, in arrears.*

**Verizon Response**

The billing start date for any product or service is the day service has been tested and accepted by Verizon and the customer. Some services such as Local Access, bill one month in advance.

This requirement should be offset by the State of West Virginia requirement of 60 day payment terms. Any services billed in advance will not be deemed late if they are held to pay in arrears.

## *15. Payment Methods*

*Vendor must accept payment by electronic funds transfer and P-Card. (The State of West Virginia's Purchasing Card program, administered under contract by a banking institution, processes payment for goods and services through state designated credit cards.)*

### Verizon Response

Verizon's preferred payment options are 1) ACH/Wire Transfer; 2) Check; and/or 3) Electronically with set-up of customer's bank account information through Verizon's online portal aka the VEC portal.

Verizon can only accept a P-Card as payment if customer sets up auto-pay with the P-Card and service charges will apply.

## *16. Taxes*

*The Vendor shall pay any applicable sales, use, personal property or any other taxes arising out of this Contract and the transactions contemplated thereby. The State of West Virginia is exempt from federal and state taxes and will not pay or reimburse such taxes.*

### Verizon Response

Verizon cannot agree to be responsible for all taxes in connection with the contract which amounts to tax inclusive pricing, as Verizon's prices do not include applicable taxes and surcharges.

Verizon will invoice and the State of West Virginia must pay applicable taxes, tax-like charges, and surcharges. Verizon will honor and apply valid exemption documentation or exemptions valid under applicable law without additional documentation.

## *17. Additional Fees*

*Vendor is not permitted to charge additional fees or assess additional charges that were not either expressly provided for in the solicitation published by the State of West Virginia or included in the unit price or lump sum bid amount that Vendor is required by the solicitation to provide.*

*Including such fees or charges as notes to the solicitation may result in rejection of vendor's bid. Requesting such fees or charges be paid after the contract has been awarded may result in cancellation of the contract.*

### Verizon Response

Verizon has read and understands.

## *18. Funding*

*This Contract shall continue for the term stated herein, contingent upon funds being appropriated by the Legislature or otherwise being made available. In the event funds are not appropriated or otherwise made available, this Contract becomes void and of no effect beginning on July 1 of the fiscal year for which funding has not been appropriated or otherwise made available.*

### Verizon Response

Verizon has read and understands.

## *19. Cancellation*

*The Purchasing Division Director reserves the right to cancel this Contract immediately upon written notice to the vendor if the materials or workmanship supplied do not conform to the specifications contained in the Contract.*

*The Purchasing Division Director may also cancel any purchase or Contract upon 30 days written notice to the Vendor in accordance with West Virginia Code of State Rules § 148-1-5.2.b.*

### Verizon Response

Verizon has read and understands.

## *20. Time*

*Time is of the essence with regard to all matters of time and performance in this Contract.*

### Verizon Response

Verizon has read and understands.

## *21. Applicable Law*

*This Contract is governed by and interpreted under West Virginia law without giving effect to its choice of law principles. Any information provided in specification manuals, or any other source, verbal or written, which contradicts or violates the West Virginia Constitution, West Virginia Code or West Virginia Code of State Rules is void and of no effect.*

### Verizon Response

Verizon has read and understands.

## 22. Compliance with Laws

*Vendor shall comply with all applicable federal, state, and local laws, regulations and ordinances. By submitting a bid, Vendor acknowledges that it has reviewed, understands, and will comply with all applicable laws, regulations, and ordinances.*

*SUBCONTRACTOR COMPLIANCE: Vendor shall notify all subcontractors providing commodities or services related to this Contract that as subcontractors, they too are required to comply with all applicable laws, regulations, and ordinances. Notification under this provision must occur prior to the performance of any work under the contract by the subcontractor.*

### Verizon Response

Verizon has read and understands.

## 23. Arbitration

*Any references made to arbitration contained in this Contract, Vendor's bid, or in any American Institute of Architects documents pertaining to this Contract are hereby deleted, void, and of no effect.*

### Verizon Response

Verizon has read and understands.

## 24. Modifications

*This writing is the parties' final expression of intent. Notwithstanding anything contained in this Contract to the contrary no modification of this Contract shall be binding without mutual written consent of the Agency, and the Vendor, with approval of the Purchasing Division and the Attorney General's office (Attorney General approval is as to form only).*

*Any change to existing contracts that adds work or changes contract cost, and were not included in the original contract, must be approved by the Purchasing Division and the Attorney General's Office (as to form) prior to the implementation of the change or commencement of work affected by the change.*

### Verizon Response

Verizon has read and understands.

## 25. Waiver

*The failure of either party to insist upon a strict performance of any of the terms or provision of this Contract, or to exercise any option, right, or remedy herein contained, shall not be construed as a waiver or a relinquishment for the future of such term, provision, option, right, or remedy, but the same shall continue in full force and effect.*

*Any waiver must be expressly stated in writing and signed by the waiving party.*

### Verizon Response

Verizon has read and understands.

## *26. Subsequent Forms*

*The terms and conditions contained in this Contract shall supersede any and all subsequent terms and conditions which may appear on any form documents submitted by Vendor to the Agency or Purchasing Division such as price lists, order forms, invoices, sales agreements, or maintenance agreements, and includes internet websites or other electronic documents.*

*Acceptance or use of Vendor's forms does not constitute acceptance of the terms and conditions contained thereon.*

### Verizon Response

Verizon has read and understands.

## *27. Assignment*

*Neither this Contract nor any monies due, or to become due hereunder, may be assigned by the Vendor without the express written consent of the Agency, the Purchasing Division, the Attorney General's office (as to form only), and any other government agency or office that may be required to approve such assignments.*

### Verizon Response

Verizon clarifies that notwithstanding the above, either party may assign this Contract or any of its rights thereunder to an affiliate or successor upon notice to the other party.

All other assignments without prior written consent are void and any written request for assignment will not be unreasonably withheld.

## *28. Warranty*

*The Vendor expressly warrants that the goods and/or services covered by this Contract will: (a) conform to the specifications, drawings, samples, or other description furnished or specified by the Agency; (b) be merchantable and fit for the purpose intended; and (c) be free from defect in material and workmanship.*

### Verizon Response

Verizon has read and understands.

## *29. State Employees*

*State employees are not permitted to utilize this Contract for personal use and the Vendor is prohibited from permitting or facilitating the same.*

### Verizon Response

Verizon has read and understands.

## 30. Privacy, Security, and Confidentiality

*The Vendor agrees that 'it will not disclose to anyone, directly or indirectly, any such personally identifiable information or other confidential information gained from the Agency, unless the individual who is the subject of the information consents to the disclosure in writing or the disclosure is made pursuant to the Agency's policies, procedures, and rules.*

*Vendor further agrees to comply with the Confidentiality Policies and Information Security Accountability Requirements, set forth in http://www.state.wv.us/admin/purchase/privacy/default.htm.*

### Verizon Response

Verizon has read and understands.

## 31. Your Submission Is a Public Document

*Vendor's entire response to the Solicitation and the resulting Contract are public documents.*

*As public documents, they will be disclosed to the public following the bid/proposal opening or award of the contract, as required by the competitive bidding laws of West Virginia Code §§ 5A-3-1 et seq., 5-22-1 et seq., and 5G-1-1 et seq. and the Freedom of Information Act West Virginia Code §§ 29B-1-1 et seq.*

*DO NOT SUBMIT MATERIAL YOU CONSIDER TO BE CONFIDENTIAL, A TRADE SECRET, OR OTHERWISE NOT SUBJECT TO PUBLIC DISCLOSURE.*

*Submission of any bid, proposal, or other document to the Purchasing Division constitutes your explicit consent to the subsequent public disclosure of the bid, proposal, or document.*

*The Purchasing Division will disclose any document labeled "confidential," "proprietary," "trade secret," "private," or labeled with any other claim against public disclosure of the documents, to include any "trade secrets" as defined by West Virginia Code § 47-22-1 et seq. All submissions are subject to public disclosure without notice.*

### Verizon Response

Verizon has read and understands.

## 32. Licensing

*In accordance with West Virginia Code of State Rules § 148-1-6.1.e, Vendor must be licensed and in good standing in accordance with any and all state and local laws and requirements by any state or local agency of West Virginia, including, but not limited to, the West Virginia Secretary of State's Office, the West Virginia Tax Department, West Virginia Insurance Commission, or any other state agency or political subdivision.*

*Obligations related to political subdivisions may include, but are not limited to, business licensing, business and occupation taxes, inspection compliance, permitting, etc.*

*Upon request, the Vendor must provide all necessary releases to obtain information to enable the Purchasing Division Director or the Agency to verify that the Vendor is licensed and in good standing with the above entities.*

*SUBCONTRACTOR COMPLIANCE: Vendor shall notify all subcontractors providing commodities or services related to this Contract that as subcontractors, they too are required to be licensed, in good standing, and up-to-date on all state and local obligations as described in this section.*

*Obligations related to political subdivisions may include, but are not limited to, business licensing, business and occupation taxes, inspection compliance, permitting, etc. Notification under this provision must occur prior to the performance of any work under the contract by the subcontractor.*

**Verizon Response**

Verizon has read and understands.

### *33. Antitrust*

*In submitting a bid to, signing a contract with, or accepting a Award Document from any agency of the State of West Virginia, the Vendor agrees to convey, sell, assign, or transfer to the State of West Virginia all rights, title, and interest in and to all causes of action it may now or hereafter acquire under the antitrust laws of the United States and the State of West Virginia for price fixing and/or unreasonable restraints of trade relating to the particular commodities or services purchased or acquired by the State of West Virginia.*

*Such assignment shall be made and become effective at the time the purchasing agency tenders the initial payment to Vendor.*

**Verizon Response**

Verizon has read and understands.

### *34. Vendor Certifications*

*By signing its bid or entering into this Contract, Vendor certifies*

*(1) that its bid or offer was made without prior understanding, agreement, or connection with any corporation, firm, limited liability company, partnership, person or entity submitting a bid or offer for the same material, supplies, equipment or services;*

*(2) that its bid or offer is in all respects fair and without collusion or fraud;*

*(3) that this Contract is accepted or entered into without any prior understanding, agreement, or connection to any other entity that could be considered a violation of law; and*

*(4) that it has reviewed this Solicitation in its entirety; understands the requirements, terms and conditions, and other information contained herein.*

*Vendor's signature on its bid or offer also affirms that neither it nor its representatives have any interest, nor shall acquire any interest, direct or indirect, which would compromise the performance of its services hereunder.*

*Any such interests shall be promptly presented in detail to the Agency.*

*The individual signing this bid or offer on behalf of Vendor certifies that he or she is authorized by the Vendor to execute this bid or offer or any documents related thereto on Vendor's behalf; that he or she is authorized to bind the Vendor in a contractual relationship; and that, to the best of his or her knowledge, the Vendor has properly registered with any State agency that may require registration.*

**Verizon Response**

Verizon has read and understands.

## *35. Vendor Relationship*

*The relationship of the Vendor to the State shall be that of an independent contractor and no principal-agent relationship or employer-employee relationship is contemplated or created by this Contract. The Vendor as an independent contractor is solely liable for the acts and omissions of its employees and agents.*

*Vendor shall be responsible for selecting, supervising, and compensating any and all individuals employed pursuant to the terms of this Solicitation and resulting contract. Neither the Vendor, nor any employees or subcontractors of the Vendor, shall be deemed to be employees of the State for any purpose whatsoever.*

*Vendor shall be exclusively responsible for payment of employees and contractors for all wages and salaries, taxes, withholding payments, penalties, fees, fringe benefits, professional liability insurance premiums, contributions to insurance and pension, or other deferred compensation plans, including but not limited to, Workers' Compensation and Social Security obligations, licensing fees, etc. and the filing of all necessary documents, forms, and returns pertinent to all of the foregoing.*

*Vendor shall hold harmless the State, and shall provide the State and Agency with a defense against any and all claims including, but not limited to, the foregoing payments, withholdings, contributions, taxes, Social Security taxes, and employer income tax returns.*

### Verizon Response

Verizon has read and understands.

## *36. Indemnification*

*The Vendor agrees to indemnify, defend, and hold harmless the State and the Agency, their officers, and employees from and against:*

*(1) Any claims or losses for services rendered by any subcontractor, person, or firm performing or supplying services, materials, or supplies in connection with the performance of the Contract;*

*(2) Any claims or losses resulting to any person or entity injured or damaged by the Vendor, its officers, employees, or subcontractors by the publication, translation, reproduction, delivery, performance, use, or disposition of any data used under the Contract in a manner not authorized by the Contract, or by Federal or State statutes or regulations; and*

*(3) Any failure of the Vendor, its officers, employees, or subcontractors to observe State and Federal laws including, but not limited to, labor and wage and hour laws.*

### Verizon Response

Verizon takes exception to the above Indemnification requirements but is open to negotiating mutually agreeable indemnity provisions in the final Agreement similar to the following.

Verizon will indemnify the Customer, its agents and employees, against any claim, loss, liability, fines, damages costs or expense for injury to or death of any persons and any loss or damage to any real or tangible property (collectively, 'Claim(s)') resulting from the negligent or other tortious acts or omissions of Verizon, its agents, representatives, employees or subcontractors, in the performance of work under this Agreement, except that Verizon, to the fullest extent permitted by applicable law, will not have any liability or responsibility to indemnify any person or entity for any such Claim(s), to the extent the same was caused by any negligent or other tortious act or omission of such person or entity.

The person or entity seeking indemnity hereunder must provide Verizon with:

(i) Prompt written notice of any such Claim, and Verizon shall have the full right and opportunity to conduct the defense of all such Claims; and

(ii) Full information and all reasonable cooperation in support of such defense, and shall have the right to participate in such defense, but no costs or expenses shall be incurred for either party by the other party without such other party's prior written consent.

## *37. Purchasing Affidavit*

*In accordance with West Virginia Code § § 5A-3-1Oa and 5-22-l(i), the State is prohibited from awarding a contract to any bidder that owes a debt to the State or a political subdivision of the State, Vendors are required to sign, notarize, and submit the Purchasing Affidavit to the Purchasing Division affirming under oath that it is not in default on any monetary obligation owed to the state or a political subdivision of the state.*

### Verizon Response

Verizon has read and understands.

## *38. Additional Agency and Local Government Use*

*This Contract may be utilized by other agencies, spending units, and political subdivisions of the State of West Virginia; county, municipal, and other local government bodies; and school districts ("Other Government Entities"), provided that both the Other Government Entity and the Vendor agree.*

*Any extension of this Contract to the aforementioned Other Government Entities must be on the same prices, terms, and conditions as those offered and agreed to in this Contract, provided that such extension is in compliance with the applicable laws, rules, and ordinances of the Other Government Entity.*

*A refusal to extend this Contract to the Other Government Entities shall not impact or influence the award of this Contract in any manner.*

### Verizon Response

Verizon has read and understands.

## 39. Conflict of Interest

*Vendor, its officers or members or employees, shall not presently have or acquire an interest, direct or indirect, which would conflict with or compromise the performance of its obligations hereunder.*

*Vendor shall periodically inquire of its officers, members and employees to ensure that a conflict of interest does not arise. Any conflict of interest discovered shall be promptly presented in detail to the Agency.*

### Verizon Response

Regarding a possible perceived conflict of interest, Melanie Lopez a former employee of Verizon, Frontier, and most recently the WV Office of Technology was recently re-hired by Verizon to fulfill the roll of a Verizon Service Manager supporting the various State of West Virginia accounts beginning November 5, 2018.

Mrs. Lopez has not participated in Verizon's response to this RFP.

Verizon believes Mrs. Lopez does not presently have an interest, direct or indirect, which would conflict with or compromise the performance of Verizon's obligations now or in the future.

## 40. Reports

*Vendor shall provide the Agency and/or the Purchasing Division with the following reports identified by a checked box below*

*_X_Such reports as the Agency and/or the Purchasing Division may request. Requested reports may include, but are not limited to, quantities purchased, agencies utilizing the contract, total contract expenditures by agency, etc.*

*_X_ Quarterly reports detailing the total quantity of purchases in units and dollars, along with a listing of purchases by agency. Quarterly reports should be delivered to the Purchasing Division via email at purchasing.regulations@wv.gov.*

### Verizon Response

Verizon has read and understands.

## 41. Background Check

*In accordance with W. Va. Code § 15-2D-3, the Director of the Division of Protective Services shall require any service provider whose employees are regularly employed on the grounds or in the buildings of the Capitol complex or who have access to sensitive or critical information to submit to a fingerprint-based state and federal background inquiry through the state repository.*

*The service provider is responsible for any costs associated with the fingerprint-based state and federal background inquiry.*

*After the contract for such services has been approved, but before any such employees are permitted to be on the grounds or in the buildings of the Capitol complex or have access to sensitive or critical information, the service provider shall submit a list of all persons who will be physically present and working at the Capitol complex to the Director of the Division of Protective Services for purposes of verifying compliance with this provision.*

*The State reserves the right to prohibit a service provider's employees from accessing sensitive or critical information or to be present at the Capitol complex based upon results addressed from a criminal background check.*

*Service providers should contact the West Virginia Division of Protective Services by phone at (304) 558-9911 for more information.*

## Verizon Response

Verizon has read and understands.

## 42. Preference for Use of Domestic Steel Products

*Except when authorized by the Director of the Purchasing Division pursuant to W. Va. Code § 5A-3-56, no contractor may use or supply steel products for a State Contract Project other than those steel products made in the United States.*

*A contractor who uses steel products in violation of this section may be subject to civil penalties pursuant to W. Va. Code § 5A-3-56. As used in this section*

*a. "State Contract Project" means any erection or construction of, or any addition to, alteration of or other improvement to any building or structure, including, but not limited to, roads or highways, or the installation of any heating or cooling or ventilating plants or other equipment, or the supply of and materials for such projects, pursuant to a contract with the State of West Virginia for which bids were solicited on or after June 6, 2001.*

*b. "Steel Products" means products rolled, formed, shaped, drawn, extruded, forged, cast, fabricated or otherwise similarly processed, or processed by a combination of two or more or such operations, from steel made by the open heath, basic oxygen, electric furnace, Bessemer or other steel making process. The Purchasing Division Director may, in writing, authorize the use of foreign steel products if*

*c. The cost for each contract item used does not exceed one tenth of one percent (.1%) of the total contract cost or two thousand five hundred dollars ($2,500.00), whichever is greater. For the purposes of this section, the cost is the value of the steel product as delivered to the project; or*

*d. The Director of the Purchasing Division determines that specified steel materials are not produced in the United States in sufficient quantity or otherwise are not reasonably available to meet contract requirements.*

## Verizon Response

Verizon has read and understands.

## 43. Preference for Use of Domestic Aluminum, Glass, and Steel

*In Accordance with W. Va. Code § 5-19-1 et seq., and W. Va. CSR § 148-10-1 et seq., for every contract or subcontract, subject to the limitations contained herein, for the construction, reconstruction, alteration, repair, improvement or maintenance of public works or for the purchase of any item of machinery or equipment to be used at sites of public works, only domestic aluminum, glass or steel products shall be supplied unless the spending officer determines, in writing, after the receipt of offers or bids,*

*(1) that the cost of domestic aluminum, glass or steel products is unreasonable or inconsistent with the public interest of the State of West Virginia,*

*(2) that domestic aluminum, glass or steel products are not produced in sufficient quantities to meet the contract requirements, or*

*(3) the available domestic aluminum, glass, or steel do not meet the contract specifications.*

*This provision only applies to public works contracts awarded in an amount more than fifty thousand dollars ($50,000) or public works contracts that require more than ten thousand pounds of steel products.*

*The cost of domestic aluminum, glass, or steel products may be unreasonable if the cost is more than twenty percent (20%) of the bid or offered price for foreign made aluminum, glass, or steel products.*

*If the domestic aluminum, glass or steel products to be supplied or produced in a "substantial labor surplus area", as defined by the United States Department of Labor, the cost of domestic aluminum, glass, or steel products may be unreasonable if the cost is more than thirty percent (30%) of the bid or offered price for foreign made aluminum, glass, or steel products.*

*This preference shall be applied to an item of machinery or equipment, as indicated above, when the item is a single unit of equipment or machinery manufactured primarily of aluminum, glass or steel, is part of a public works contract and has the sole purpose or of being a permanent part of a single public works project.*

*This provision does not apply to equipment or machinery purchased by a spending unit for use by that spending unit and not as part of a single public works project.*

*All bids and offers including domestic aluminum, glass or steel products that exceed bid or offer prices including foreign aluminum, glass or steel products after application of the preferences provided in this provision may be reduced to a price equal to or lower than the lowest bid or offer price for foreign aluminum, glass or steel products plus the applicable preference.*

*If the reduced bid or offer prices are made in writing and supersede the prior bid or offer prices, all bids or offers, including the reduced bid or offer prices, will be reevaluated in accordance with this rule.*

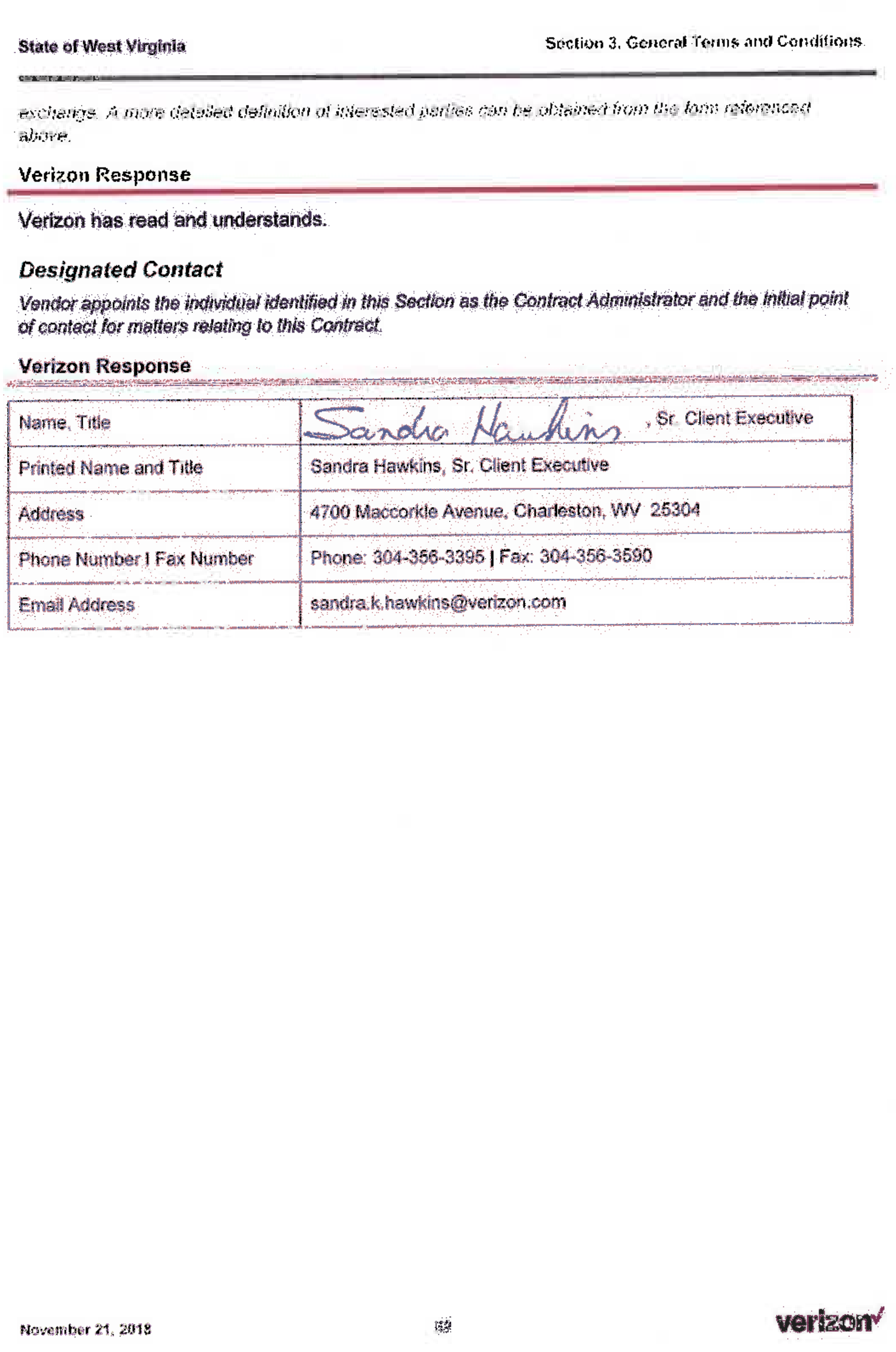
**Verizon Response**

Verizon has read and understands.

## *44. Interested Party Supplemental Disclosure*

*W. Va. Code § 6D-I -2 requires that for contracts with an actual or estimated value of at least $1 million, the vendor must submit to the Agency a supplemental disclosure of interested parties reflecting any new or differing interested parties to the contract, which were not included in the original pre- award interested party disclosure, within 30 days following the completion or termination of the contract.*

*A copy of that form is included with this solicitation or can be obtained from the WV Ethics Commission. This requirement does not apply to publicly traded companies listed on a national or international stock*



*exchange. A more detailed definition of interested parties can be obtained from the form referenced above.*

### Verizon Response

Verizon has read and understands.

### *Designated Contact*

*Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.*

### Verizon Response

| | |
|---|---|
| Name, Title | Sandra Hawkins , Sr. Client Executive |
| Printed Name and Title | Sandra Hawkins, Sr. Client Executive |
| Address | 4700 Maccorkle Avenue, Charleston, WV 25304 |
| Phone Number I Fax Number | Phone: 304-356-3395 \| Fax: 304-356-3590 |
| Email Address | sandra.k.hawkins@verizon.com |

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through wvOASIS, I certify that I have reviewed this Solicitation in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that I am authorized by the vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

Verizon Business Network Services Inc. on behalf of MCI Communications Services, Inc. dba Verizon Business Services
(Company)

Adam S. Davis, Sr. Manager, Billing
(Authorized Signature) (Representative Name, Title)

Adam S. Davis, Sr. Manager - Billing
(Printed Name and Title of Authorized Representative)

November 20, 2018
(Date)

Phone: 304-356-3395 | Fax: 304-356-3590
(Phone Number) (Fax Number)

## *Definitions, Abbreviations, Acronyms*

*1. ANI, Automatic Number Identification*

*2. CoS, Class of Service*

*3. DID, Direct Inward Dial*

*4. DNIS, Dialed Number Identification Service*

*5. E.164, the international public telecommunication numbering plan*

*6. High Security, any use case where the Vendor's solution requires a higher security baseline standard. High security use cases are either the result of regulatory or legal compliance requirements and/or risk assessment indicates a higher level of security is warranted.*

*7. ID, Identification*

*8. IP, Internet Protocol*

*9. LAN, Local Area Network*

*10. LMS, Learning Management System*

*11. MIS , Millisecond*

*12. MACD, Move, Add, Change, Delete*

*13. Microsoft 0365, Microsoft Office 365*

*14. MPLS, Multiprotocol Label Switching*

*15. MWI, Message Waiting Indicator*

*16. PHI, Protected Health Information*

*17. PIIT, Personally Identifiable Information*

*18. PMBOK, Project Management Body of Knowledge*

*19. PMO, Project Management Office*

*20. POTS, Plain Old Telephone Service*

*21. PRI, Primary Rate futerface*

*22. PS/ALI, Private Switch/Automatic Location Identifier*

*23. PSAP, Public Safety Answering Point*

*24. PSTN, Public Switched Telephone Network*

*25. QoS, Quality of Service*

*26. SIP, Session Initiation Protocol*

*27. SOW, Statement of Work*

*28. SRST, Survivable Remote Site Telephony*

*29. Standard Security, any use case where the Vendor's solution does not require heightened security baseline standards. The standard security use case is delineated to provide the State a potentially lower cost option when a standard level of security provides an appropriate level of protection.*

*30. TCR, Telecommunications Change Request*

31. *UCaaS, Unified Communications as a Service*
32. *UCCaaS, Unified Communications and Collaborations as a Service*
33. *VCC, Virtual Contact Center*
34. *VLAN, Virtual Local Area Network*
35. *VoIP, Voice over Internet Protocol*
36. *WAN, Wide Area Network*
37. *WBS, Work Breakdown Structure*
38. *WVOT, West Virginia Office of Technology*

### Verizon Response

Verizon has read and understands.

# Section 4. Project Specifications

## *4.1. Background and Current Operating Environment*

*As outlined in the West Virginia State Code §5A-6-4e "the Chief Technology Officer shall oversee telecommunications services used by state spending units for the purpose of maximizing efficiency to the fullest possible extent".*

*Additionally, per State Code §5A-6-4a (11), the Chief Technology Officer develops a "unified and integrated structure for information systems for all executive agencies."*

*In pursuance of those objectives, the West Virginia Office of Technology is seeking proposals from Vendors to establish an open-end, Statewide Contract for Managed Voice Services and Hosted Voice over Internet Protocol ("VoIP") Services, encompassing Unified Communications as a Service ("UCaaS"), and Hosted Contact Center Services.*

*It is the State's intent to establish a contract with a single Vendor to provide maintenance, management, and support for the State's current IP Telephony platforms while working to migrate those telephony services to a fully managed and hosted VoIP solution.*

*Additionally, the Vendor will be expected to provide daily management and operational support for multiple Contact Centers while working to migrate those Contact Centers to its hosted solution.*

*Currently, the State of West Virginia has an estimated 10,000 phones on multiple Cisco VoIP solutions - 3x Cisco Unified Call Manager and Unity Express, 4x Cisco Unified Call Manager and Unity, 7x Cisco Unified Call Manager and Unity Connection, lOx Cisco Unified Call Manager and Unity Connection, Cisco Call Manager Express, ten (10) Cisco Contact Center Version 7 sites, and a Hosted VoIP Solution with Verizon Business Solutions (UCCaaS and Contact Center); it is anticipated all of those sites currently utilizing a VoIP solution will be migrated to the Vendor's proposed hosted solution.*

*In addition to the current VoIP Agencies, the State also requires the flexibility to implement a VoIP solution at sites where one does not currently exist. Potentially, the State may leverage the awarded contract to implement another estimated 10,000 users where traditional telephony services exist.*

*The State of WV' s current environments consist of the following:*

- *Cisco Unified Messaging*
- *Cisco Unity*
- *Cisco Unity Connection*
- *Cisco Unity Express*
- *Cisco Call Manager Express*
- *Cisco Contact Center Express*
- *Cisco Expressway C&E*
- *Cisco Presence*
- *Cisco Jabber*
- *Cisco Gateways using VoIP Session Initiation Protocol ("SIP") Trunks, Primary Rate Interface ("PRis") Circuits, and Analog POTS ("Plain Old Telephone Service") lines*
- *Microsoft Skype for Business 2016*

- *Microsoft Active Directory*
- *Microsoft Office 365*
- *Cisco Survivable Remote Site Telephony ("SRST")*
- *Bridge Communications Operator Console*
- *Singlewire Informacast Paging*
- *Verizon hosted solution- Unified Communications and Collaborations as a Service (UCCaaS)*
- *Verizon hosted solution - Virtual Contact Center (VCC)*

*More information regarding the State's current telephony infrastructure can be found in Appendix A.*

*Meanwhile, the State's current Wide Area Network ("WAN") is undergoing a conversion from Switched Ethernet to Multiprotocol Label Switching ("MPLS") services, which may impact how the Vendor's proposed solution will be implemented.*

*The WVOT is working with Verizon Business to migrate an estimated 500 data circuits across the State with a projected completion of December 2018. Thus far, approximately 275 circuits have been migrated, meaning that the proposed VoIP solution may be implemented at those sites using MPLS circuits to ensure quality of service.*

*The State has deployed Cisco routers for WAN communications. Local Area Networks ("LANs") are comprised of various switches manufactured by Cisco, Hewlett Packard, Brocade, and Extreme.*

### Verizon Response

Verizon has read and understands.

## 4.2. Project Goals and Mandatory Requirements

*The State of West Virginia is seeking to establish a contract with a Vendor for the management of the State's current Legacy Environment and to migrate its Legacy Environment to a Hosted VoIP Solution, including Contact Center Services.*

*Vendor should describe its approach and methodology to providing the service or solving the problem described by meeting the goals/objectives identified below. Vendor's response should include any information about how the proposed approach is superior or inferior to other possible approaches as well as identify areas where the proposed solution exceeds the project expectations.*

*4.2.1. Goals and Objectives - The project goals and objectives are listed below.*

*The project goals and objectives are listed below.*

*4.2.1.1 Voice Services*

*4.2.1.1.1 Managed Voice Services - Support of State's Legacy IP Environment*

*4.2.1.1.1.1 The State's goal is to contract with a single Vendor for all application, hardware, and MACD management, maintenance, and support of its current IP Telephony platforms (as described in Appendix A), with the goal of the Vendor migrating the State's current IP telephony infrastructure, excluding network infrastructure, to a unified, hosted IP platform within 24 months.*

*The State further desires an economical monthly per phone cost for these support services. As such:*

*The State is proposing the following division of duties for the support of its Legacy IP Environment:*

*Vendor Duties:*

*1. Create an operational plan of the State's Legacy IP Environment for the State's review and approval*

## Verizon Response

Verizon has read and understands.

*2. Daily management, operational support, and ongoing maintenance of the State's current telephony environment, as outlined in Appendix A.*

## Verizon Response

Verizon plans to utilize the current TEKsystems' contractors provided to the State to deliver local onsite support for the Legacy IP systems.

Verizon has read and understands as:

- Support of the Legacy IPPBX systems as currently designed with no changes to the design or architecture.
- Table 1.1 indicates 214 Sites, 10,000 stations spread across the Legacy CUCM and CME/CUE clusters.
- The State of West Virginia's WAN is not in scope for Verizon's support in this RFP.

*3. MACD changes to the State's current telephony infrastructure.*

## Verizon Response

Verizon has read and understands.

*4. Replacement of failed parts where feasible, outdated telephony equipment, or other telephony components. If the Vendor is unable to furnish parts or replace equipment, the State expects the Vendor to migrate that site to the Vendor's Hosted VoIP platform.*

## Verizon Response

Verizon support services will engage with reasonable effort to locate replacements of failed hardware.

Some inventory may be end of life/end of support. If the hardware is not available for purchase from our suppliers, we would need to work with the State of West Virginia on a workaround solution to solve the problem for the user.

As soon as it has been determined that the part(s) cannot be sourced, Verizon will escalate the issue to the State of West Virginia. Based on the needs of the business unit, Verizon and the State of West Virginia will decide which hosted platform we would migrate the users to.

Site specific variables and requirements will dictate the amount of time needed to get our hosted platform provisioned and CPE ordered if required.

*5. Set-up mutually agreed upon standing meetings with the State to address concerns, changes, service interruptions, and project progress.*

## Verizon Response

Verizon has read and understands.

*6. The Vendor should alert the State points of contact after being notified of any service interruptions, in writing, that exceed sixty (60) minutes. The Vendor should provide updates to the State every sixty (60) minutes thereafter until the issue is resolved .*

## Verizon Response

Verizon has read and understands.

*7. The Vendor should have a 24x7x365 operations center that includes Tier 1 support to receive trouble tickets and onsite operational support for critical failures.*

## Verizon Response

Verizon has read and understands the premise based management requirements. Verizon has 24x7x365 network operations support for our customer's needs. Verizon will be acting on behalf of the State of West Virginia for the IP PBX systems in which the State already has support contracts on.

At the end of the support term (not to exceed the 24 month transition), Verizon will assume operational support (including maintenance) of the IP PBX servers that are not End of Life/End of Support. If the problem requires onsite remediation, we will dispatch a tech onsite to work the problem.

The onsite support will be 24x7, 4 hour response. Verizon plans to utilize the current TEKsystems' contractors provided to the State to deliver local onsite support for the Legacy IP systems.

*State Duties:*

*1. Management of State's LAN/WAN Network Infrastructure*

*2. Ordering, disconnecting, and billing services*

## Verizon Response

Verizon has read and understands.

*4.2.1.1.1.2 The State desires the Vendor provide the State with its proposed Operations Plan within 30 calendar days of contract effective date, outlining its plan for managing, supporting, and maintaining the State's current IP telephony infrastructure .*

*The Vendor's Operations Plan should include a strategy for assuming its duties, as outlined above. Please describe your company's experience and strategy in developing operations plans for supporting legacy environments.*

## Verizon Response

Verizon has read and understands.

Using the ITIL framework, we use a defined delivery management process for the execution of all services being requested in this RFP. Our philosophy is to prioritize our communication plan and to be as transparent as possible during the lifecycle of the contract.

As part delivery management process, a Delivery Manager (DM) will be assigned to the State of West Virginia engagement to oversee critical success factors, coordinate communication with client teams and SMEs, and to ensure a smooth and productive engagement that meets client expectations.

Each Delivery Manager is a full-time member of our delivery organization and is trained extensively in the methods, processes, and tools required to efficiently managing complex engagements.

During the first 30 days, we will work within the Discovery Phase of our framework.

Verizon will work with State of West Virginia, the various business segments, existing Verizon technicians supporting State of West Virginia and the Service Desk (as needed) to capture all pertinent policy, process, knowledge articles and documentation, as well as perform the identification of existing gaps that require emphasis and content development during the remainder of transition.

During Discovery, the Verizon team will meet with key State of West Virginia member(s) to gain insight into the existing operations, teams, and support expectations.

The result of these finding will be used to build an Operations Plan for the project.

*4.2.1.1.1.3 The State desires that the State and Vendor formalize and agree upon an Operations Plan within 60 calendar days of contract effective date for the management, support, and maintenance of the State's current telephony infrastructure.*

*Please describe your company's ability to deliver the finalized Operations Plan to the State within 60 calendar days of contract effective date with scheduling the appropriate meetings, making changes after State input, and meeting deadlines.*

## Verizon Response

The Verizon Program Management Office and our Delivery Manager will work with the State of West Virginia to finalize the Operations Plan according to the required deadlines.

Our Delivery Manager will be in continual communication with your project sponsor to garner insight into customer satisfaction throughout this project.

At any time, if an issue is identified either by your team or ours, we follow our continual service improvement model to remedy the situation and return the engagement to our high standards for customer satisfaction.

As part of our Project Management Lifecycle and best practices, the Delivery Manager will provide the State of West Virginia with status reports provided at an agreed upon timeframe.

The report can be presented via email or we can establish a weekly meeting with the State of West Virginia's stakeholders, if that is requested.

This would give the State of West Virginia a regularly scheduled forum to provide feedback to our project team for continual improvement opportunities.

*4.2.1.1.1.4 The State desires the Vendor to be fully managing its Legacy Environment within 90 calendar days of contract effective date and until all sites wishing to adopt these services have been migrated to a Hosted VoIP solution.*

*Please describe your company's experience in providing support of a Legacy Environment, its experience in taking over existing infrastructure, and provide a plan showing how this goal can be met.*

## Verizon Response

Verizon has an experienced Service Desk practice area that has been operating for over 20 years and is specialized in providing complete Service Desk, team based solutions.

Many of our Service Desk customers are faced with a multitude of challenges associated with managing multiple staffing vendors, maintaining a predictable support budget, service inconsistencies and managing Service Desk attrition and the associated impacts to support.

Our Service Desk offering provides a unique and flexible approach to these challenges in that we work with our customers to offer a variety of solutions to meet specific customer needs and requirements.

The Verizon Transition and Implementation Plan consists of a two (2)-phased approach, as outlined below:

### Discovery Phase

The Discovery Phase is a process that begins with defining the transition schedule, performing an in-depth onsite assessment including: interviews with the key stakeholders, managers, and business owners.

Engaging in a deep dive into existing operations including current and past incident data for trending and benchmarking. Evaluation of standard operating procedures and current knowledgebase content. Identify existing reports and establish criteria for future reporting needs.

- Initiate transition kickoff meeting; identify transition schedule and site visit schedule
- Interview State of West Virginia resources (current leadership, technology manager, primary business owners)
- Begin recruiting process for candidates to fill open positions on the delivery team
- Evaluate existing IT Support operations, including standard operating procedures
- Review and assess current knowledgebase content, past incident data for trending and benchmarking
- Identify existing reports; establish criteria for future reporting needs

### Implementation Phase

Implementation is the phase prior to service going live. During the implementation phase we focus on building the right team with the right cultural and skill fit. We implement updated standard operating procedures into the onboarding and training processes.

Changes and modifications are made to the existing knowledgebase and incident management system. Incident, interaction, and trend reporting needs are implemented. Recurring dates for weekly and monthly status meetings and measurement reviews are established with the client, and the new hire training program (classroom and shadowing) are completed.

- Recruit, test, interview and hire new resources to join the delivery team
- Implement updated standard operating procedures into onboarding and training process
- Implement any required changes / modifications to the existing knowledgebase
- Establish recurring dates for weekly and monthly status meetings and measurement reviews with State of West Virginia key stakeholders
- Facilitate new hire training program for all newly acquired resources (training and shadowing of existing teams)
- Prepare for service transition and Go-Live

Upon the completion of the service transition, Verizon will Go-Live with the delivery of services to State of West Virginia.

*4.2.1.1.1.5 It is the State's desire that the awarded Vendor of this contract will establish a local support system to continue support and maintenance of the State's Legacy IP systems. Please describe your company's ability to provide maintenance and support of the State's Legacy Environment.*

## Verizon Response

Verizon has read and understands the premise based management requirements. Verizon has 24x7x365 network operations support for our customer's needs.

Verizon will be acting on behalf of the State of West Virginia for the IP PBX systems in which the State already has support contracts on.

At the end of the State's current support term, Verizon will assume operational support (including maintenance) of the IP PBX servers that are not End of Life/End of Support (not to exceed the 24 month transition).

If the problem requires onsite remediation, we will dispatch a tech onsite to work the problem. The onsite support will be 24x7, 4 hour response.

The account team will consist of an overall lifecycle project manager, a service program manager, client executive, solutions architect in addition to our NOC managed services team. Verizon plans to utilize the current TEKsystems' contractors provided to the State to deliver local onsite support for the Legacy IP systems.

*4.2.1.1.1.6 The State desires all application, hardware, and MACD support for the State's current telephony infrastructure will be entered via the Vendor's self-service web portal and/or a Vendor-provided toll-free number within 90 calendar days from contract effective date.*

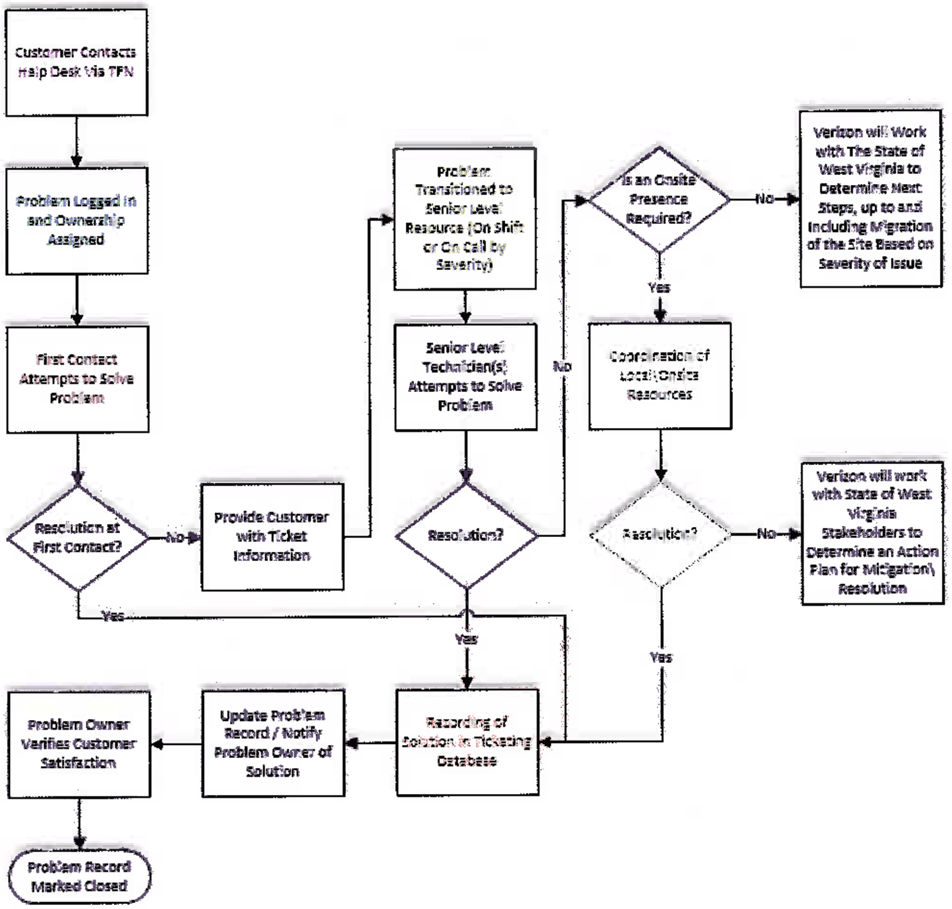
*If the Vendor determines that an issue or problem falls within the State's purview, the Vendor should notify the State's points of contact in writing within one hour of reaching this determination. Please describe your company's support offerings or its ability/plan to accomplish this.*

## Verizon Response

Verizon has read and understands.

During the Discovery Phase, Verizon will work with The State of West Virginia to determine the best process for receiving and communication on tickets. An Example of a Potential high level work flow could be as follows.

Example of possible Call Flow for State of West Virginia


Customer Contacts Help Desk Via TFN
Problem Logged in and Ownership Assigned
First Contact Attempts to Solve Problem
Resolution at First Contact?
No
Provide Customer with Ticket Information
Yes
Problem Transitioned to Senior Level Resource (On Shift or On Call by Severity)
Senior Level Technician(s) Attempts to Solve Problem
Resolution?
No
Yes
Is an Onsite Presence Required?
No
Verizon will Work with The State of West Virginia to Determine Next Steps, up to and Including Migration of the Site Based on Severity of Issue
Yes
Coordination of Local\Onsite Resources
Resolution?
No
Verizon will work with State of West Virginia Stakeholders to Determine an Action Plan for Mitigation\ Resolution
Yes
Recording of Solution in Ticketing Database
Update Problem Record / Notify Problem Owner of Solution
Problem Owner Verifies Customer Satisfaction
Problem Record Marked Closed

During the Discovery Phase leading into Implementation Verizon will work with the State of West Virginia on communication strategies and finalize designated points of contact.

*4.2.1.1.2 Transition from the State's Legacy IP Environment to the Vendor's Hosted Solution*

*4.2.1.1.2.1 The State desires all sites listed in Appendix A be migrated to a Hosted VoIP solution within 730 calendar days from contract effective date. The State reserves the right to reprioritize this list as necessary. Please describe your company's plan to accomplish these migrations.*

## Verizon Response

Please reference the Sample Project Plan provided in Appendix G of this proposal.

*4.2.1.1.2.2 The Vendor should include site preparation and coordination services to implement a tum-key solution at various State locations, including simultaneous deployments to the Vendor's hosted solution. These services should be provided by Vendor personnel knowledgeable in both the Vendor's solution and legacy public switched telephone services.*

*The State desires the Vendor perform site assessment and readiness work for the implementation of its hosted solution, at no additional cost, including a proposed division of duties (Vendor, State), which results in a Statement of Work for each site, as follows:*

*VENDOR duties:*

- *Gather site's end-user data in order to get site ready for Vendor 's hosted solution;*
- *Provide list of equipment/specifications needed for site readiness, including cabling infrastructure requirements;*
- *Conduct review to move, at a minimum, existing telephony system to new environment;*
- *Provide the State with necessary ordering information for TCRs;*
- *The State owns all data gathered under the scope of the contract and is able to obtain copies of all configuration files gathered as part of this contract. The Vendor should update, maintain the data repository in a manner negotiated with the State upon award, and provide information upon request in an Excel or csv format;*
- *Configure, tag, label, and drop-ship phones to site;*

*STATE duties:*

- *Confirm site readiness ;*
- *Coordinate between the Agency, Vendor, and other applicable parties;*
- *Purchase, configure, update and refresh network hardware;*
- *Prepare, process, and submit TCR to Vendor based on information provided ;*
- *Place physical phones*

*The Vendor should describe its solution's capability to meet or exceed each of these objectives.*

## Verizon Response

Verizon has read and understands.

# Site Survey

**(Each Site Needs a Site Survey Form Complete)**
**(Call with WVOT must occur before Site Survey to review customer environment)**

Date: ____________________
Surveyed By: ____________________ Surveyed By: ____________________
Phone Number: ____________________ Phone Number: ____________________

## *General Site Information*

Office Name: ____________________

Business Street Address: ____________________

MPOE Street Address: ____________________

Site Contact: ____________________ Phone: (   ) ____________________

Co-locate with: ____________________

Facilities Representative: ____________________

On Site Support Staff: ____________________

## *Proposed Circuit Configuration –*

Circuit Type/Speed: ____________________

Gold CAR: ____________________

## *Proposed Service Configuration:*

Site Size – 1 to 24 Sets ____
Site Size – 25 to 240 Sets ____
Site Size – 241 to 480 Sets ____
Site Size – 481+ Sets ____ Total Number of Sets at Site ______

Overhead Paging System: Make, Model, Type, Interface (FX0 or FXS) and setup?
____________________
____________________

Analog Set Requirements (FAX, ringdown, door, outside the building):
____________________
____________________

**Proposed Users Per Closet (IDF) and MDF (Standalone Only):**
1.) MPOE (name/location/Dmarc extension needed?) ____________________
2.) MDF (name/location/# of sets) ____________________

3.) IDF#1 (name/location/# of sets) ______________________________
4.) IDF#2 (name/location/# of sets) ______________________________
5.) IDF#3 (name/location/# of sets) ______________________________
6.) IDF#4 (name/location/# of sets) ______________________________
7.) IDF#5 (name/location/# of sets) ______________________________
8.) IDF#6 (name/location/# of sets) ______________________________
9.) IDF#7 (name/location/# of sets) ______________________________
10.) IDF#8 (name/location/# of sets) ______________________________

### *Existing Site Circuit and Wiring Information*

| Task Description | | Comments |
|---|---|---|
| Where is the "current" Telco equipment located; inside or outside of the MPOE or telecom room? | | |
| Explain, provide photo | | |
| Is the MPOE separate from Telecom room (Y/N)? | | |
| If yes, is there conduit between MPOE and Telecom Room? List size (number of pairs) and type (Multi-Mode/Single Mode). (Y/N, un sure)? Provide photos | | |
| Is there conduit between Telecom Rooms and wiring closets (IDF)? List size and type. (Y/N, unknown)? Provide photos | | |
| If yes is there fiber/copper pulled between the MPOE, Telecom & wiring closets (IDF) ? List size (number of pairs) and type (Copper/Multi-Mode/Single Mode). (Y/N, unknown)? Provide photos | | |
| If yes with fiber, what is connector type? (Y/N, unknown)? Provide photos | | |
| Is there a backboard with available space (3'x3'min)? | | |

## *Rack Space*

| Task Description | | Comments |
|---|---|---|
| Is there existing space for new network equipment (Router, Switch(s), Digi, and Modem)(Y/N)? Please refer to rack space estimates page 4. | | |
| If "Yes" Explain, provide photo | | |
| Is there existing space for new network or equipment if the equipment was relocated in the existing telecom racks (Y/N)? | | |
| If "Yes" Explain, provide photo | | |
| Are there any other options (.i.e., new racks, different closet, etc?) (Y/N)? | | |
| Is space available for a new Verizon Rack(s) (Must be at least 23" wide) (Y/N)? | | |
| Identify location of Verizon Rack(s) and Marked (Y/N)? | | |
| Identify location of Rack Power (Y/N)? | | |
| If there is no room for new racks in the Telecom rooms, then is there space elsewhere in the building? | | |
| If "Yes" Explain, provide photo | | |
| Any other modifications required (Y/N)? | | |

| | | |
|---|---|---|

## *Facilities Information*

| Task Description | | Comments |
|---|---|---|
| Does site have a current floor plan (Y/N)? | | |
| If yes, obtain copy from site contact and include in site survey packet. | | |

## *Telecom Closets (Complete if multiples are required)*

| Task Description | Y/N | Comments |
|---|---|---|
| If multiple Telecom rooms exist, Is there interconnectivity between closets via copper/fiber? List size (number of pairs) and type (Multi-Mode/Single Mode)? If fiber, what is connector type?<br>(Y/N, unknown)? Provide photos | | |
| Are Telecom rooms on separate Floors (Y/N)?<br>If "Yes" are they interconnected via fiber/copper? List size (number of pairs) and type (Copper/Multi-Mode/Single Mode)? If fiber, what is connector type?<br>(document location of Telecom rooms) | | |
| Does the Telecom Room need cleaning (Y/N)? Explain<br>Provide photos | | |
| Do the patch panels require clean up (Y/N)? Explain<br>Provide Photos | | |
| Any other modifications required (Y/N)? | | |
| | | |

## *Telecom Closet Inspection Notes:*

## HVAC

| Task Description | | Comments |
|---|---|---|
| Does the Telecom Room have its own HVAC unit (Y/N)? | | |
| Does it appear to be adequate? (Y/N) | | |
| Any HVAC modifications required (Y/N)? | | |
| If so explain | | |
| Are the telecom rooms operating between 40 degree F and 100 degree F with 20% to 50% relative humidity (Y/N, unsure)? | | |

## Electrical

| Task Description | Existing | Proposed |
|---|---|---|
| Document existing electrical outlets per rack (MDF and IDFs): If multiple IDF's are found, please use separate sheets of paper to populate additional IDF information. | | |
| Document existing electrical outlets on walls: | | |
| UPS Provided? (Y/N) | | |
| Any other modifications required (Y/N)? | | |

## Grounding

| Task Description | | Comments |
|---|---|---|
| Is there an existing # 6 solid ground wire in place (note: it cannot be a water pipe) (Y/N, unsure)? | | |
| If "Yes" Explain, provide photo | | |
| If "No", Mark location for new ground service and provide photo | | |
| Any other modifications required (Y/N)? | | |

## Cabling

| Task Description | | Comments |
|---|---|---|
| Does the site need additional cabling (Y/N)? | | |
| If "Yes" Explain | | |
| Does the exiting cabling need be cleaned up (Y/N)? | | |
| If "Yes" Explain, provide photo | | |

## Rack Space Estimate

| Description | Rack U's | Power Plugs |
|---|---|---|
| Router Cisco 3900 (per device) | 3 U | 2 |
| Router Cisco 2900 (per device) | 2U | 2 |
| Switch (per device) | 2U | 1 |
| Shelf for Router Management Modem (per device) | 2 U | 1 |
| Analog Gateway | 1 U | 1 |

**UCCaaS Design Questions for End User Implementation to support the data collection workbook.**

- Please provide a location list with full street addresses
- For each location, please provide:
    - Number of users with single phone and voice mail
    - Number of users requiring soft phone capability only
    - Number of users requiring physical phone and soft phone
    - Number of users requiring Expressway for MRA
    - Number of unassigned phones (hallway, conference room, etc.)
    - Number of Voice Mail only mailboxes (no phone associated with mailbox)
    - Number of new DIDs
    - Number of existing DIDs to be ported
- Are all locations VoIP ready?
- Number of hunt groups by location
    - Are any members of the hunt groups off net? If so, how many?
- Number of auto attendants by location
- Attendant Console required?
- Do you plan to use Extension Mobility? If so, how many phones?
- Do you plan to use Device Mobility?
- Do you plan to use SRST at each site in case of loss of connectivity to the UCCaaS data centers? If so, describe the connectivity for each location (quantity, type of calls allowed, etc.)
- Do any locations require a phased install?
- Do you need to display a number for outbound Caller ID that is not one of your DIDs (e.g. toll free number)? If so, how many?
- Do you plan to integrate a contact center with UCCaaS? If so, please describe.
- Do you plan to integrate with a call recording system? If so, please describe.
- Do you have any Telepresence or other video systems you wish to integrate with UCCaaS? If so, please describe.
- Do you require Integration with Call Accounting software?
    - Note: Customer provided server required
- What is the maximum number of simultaneous calls do you expect to need for each location?
- Is end user training required?

*4.2.1.1.3 Hosted Voice Services*

*The State's goal is to obtain a reliable, customizable, and scalable UCaaS solution providing hosted voice-over-IP (VOiP) services for an estimated 10,000 state employees located at various sites throughout the State. The State desires these services be provided at no additional cost, except where noted in this section. To that end:*

*4.2.1.1.3.1 The Vendor's solution should offer four voice packages.*

*The Vendor's solution should offer four voice packages. These packages should include: A Basic Package with at least Ad Hoc Conferencing, Call Forwarding, Call History, Call Hold, Call Waiting, Caller ID, and Do Not Disturb; an Enhanced Package including at least all features in the Basic package plus Voice Mail (including Immediate Divert to Voicemail and Message Waiting Indicator); a Premium Package including at least all of the features in the Enhanced Package plus Extension Mobility; and an Analog line option.*

*All packages should be available with high and standard security options. Equipment for the analog line package will not be required for this contract. Please describe your Company's offerings.*

## Verizon Response

Verizon's High Security Hosted Voice offers 2 packages: Common Space users and Named Users.

- The Common Space user package aligns with 2 of the State of West Virginia's required packages for Basic and analog users.
- The Named User package aligns with the State of West Virginia's required packages for Enhanced and Premium users.

Verizon's High Security Hosted Voice provides UC&C services such as call control, integrated/unified voicemail, presence, and conferencing.

By delivering these core Unified Communications services from its secure data centers, Verizon is able to provide and manage the UC&C capabilities using a flexible users Communications Manager virtualized application portfolio, providing the State of West Virginia with the security benefits of dedicated applications and the convenience and cost benefits of a hosted environment.

Verizon's High Security Hosted Voice for Government service uses a consumption model and charges monthly recurring fees based on the number of users and the applications and features used.

Based on the required feature sets, Agencies select the Package required for each end user or group of end users which have been aligned below with the State of West Virginia's End user package requirements.

Each package is allocated a number of allowed endpoints. "Endpoints" are defined as physical devices, mobile clients, PC-based soft clients, or integration with third party client software.

## Package Descriptions

- **Communicator**: Perfect for economizing—common area phones, break room phones, etc. where voice calling is the primary objective. This package would fit all of the State of West Virginia's Package requirements for Basic, Enhanced, Premium, and analog users.

  Upon discovery, additional capabilities are available that can meet user requirements. Pricing for these packages will be available upon request.

- **Advanced Communicator**: All features in Communicator also have access to the Jabber application, IM/P, video capabilities, Expressway MRA for mobility, iOS and Android calling and up to ten endpoints.

  This package provides many features for a low price point, especially for a mobile phone or PC Jabber client user and is available as an optional for additional cost and can be provided Discovery.

- **Collaborator**: All services in Advanced Communicator as well as FedRAMP WebEx for up to 8 internal participants. This package is available as an optional for additional cost and can be provided Discovery.

- **Advanced Collaborator**: All services in Advanced Communicator as well as FedRAMP WebEx for up to 200 internal and external participants. This package is available as an optional for additional cost and can be provided Discovery.

All packages exclude PSTN services, B2B video calling and all end points, hard phone or client, must support FIPS 140-2 encryption.

| | Communicator | Advanced Communicator | Collaborator | Advanced Collaborator |
|---|---|---|---|---|
| Voice Call Control | X | X | X | X |
| Voice Messaging | X | X | X | X |
| Instant Messaging and Presence | | X | X | X |
| Video Call Control | | X | X | X |
| Mobility | | X | X | X |
| Emergency Call Handling | X | X | X | X |
| # Supported endpoints | 1 | 10 | 10 | 10 |
| Supported devices | FIPS 140-2 compliant IP Phones | FIPS 140-2 compliant IP Phones and Jabber client | FIPS 140-2 compliant IP Phones and Jabber | FIPS 140-2 compliant IP Phones and Jabber client |

| | Communicator | Advanced Communicator | Collaborator | Advanced Collaborator |
|---|---|---|---|---|
| | | (PC and mobile devices) | client (PC and mobile devices) | (PC and mobile devices) |

All packages include Emergency Call Handling using the native CUCM emergency call routing feature. The Emergency Call Handling feature helps you to manage emergency calls in your telephony network while following local ordinances and regulations.

All packages Advanced Communicator and above (not Communicator) include Expressway Mobile Remote Access (MRA) for mobility. Expressway MRA enables secure, VPN-less access to mobile Jabber.

### Optional Features

Users may select the following features, or add them to a Primary Capability Package. Where noted, a feature may be required with other packages or capabilities. If upon discovery these optional features are required, additional charges may apply.

- **Additional Storage**: Additional storage for WebEx conference recordings. Available in conjunction with the Advanced Collaborator package. Available in 1 GB increments to expand the default 1 GB of storage available. Once the allocated storage limit has been reached, no further data may be stored until space is freed up.
- **Add-on Audio Conferencing**: Flat-rate audio subscription plan as an add-on to the Advanced Collaborator package. Each entitled user has unlimited access to Domestic call-in services.

  Must be ordered in a quantity equal to the Advanced Collaborator subscription quantity, cannot be mixed with Add-on Audio Conferencing with Callback.
- **Add-on Audio Conferencing with Callback**: Flat-rate audio subscription plan as an add-on to the Advanced Collaborator package. Each entitled user has unlimited access to Domestic call-in and Domestic call-back services.
- Note: Must be ordered in a quantity equal to the Advanced Collaborator subscription quantity, cannot be mixed with Add-on Audio Conferencing.
- **Integration**: Custom integration with Agency systems. Supports Agency defined requirements on an individual case basis.
- **Local survivability**: Provides local survivability in the event of a WAN failure. Limited functionality is supported; specific capabilities are dependent on defined solution. Available on an individual case basis.

Verizon's UCCaaS Monthly Recurring charges include:

- Software/Features as defined in the Package definitions
- Standard implementation and infrastructure support within the data center
- Maintenance on all data center elements
- Right to new software upgrades when Verizon makes available
- 24x7x365 Fault Management including restoration and patch management
- Configuration or change management
- Security Administration
- Inventory Tracking (data-center based)
- Lifecycle Management Customer Empowerment
- Performance Reporting
- Utilization Reporting
- Self-administration Moves, Adds, Changes, and Deletes (MACD) capabilities
- Verizon-supported administrative MACD support

*4.2.1.1.3.2 The State desires six handset options for use under this contract: a 2-line phone, a 5-line phone with sidecar capabilities, a conference phone, a softphone, a wireless phone, and an ADA-compliant hardware option.*

*The State further desires a leasing option for all handsets on this contract, by which the State will pay a monthly lease price to be added to the price of the monthly voice package. In the event that a phone is broken or stops functioning, the State desires the Vendor replace that phone, at no additional cost.*

*Additionally, the State desires that the Vendor refresh equipment in-line with the Original Equipment Manufacturer's refresh program, at no additional cost. At the end of the contract, the State will own all of the phones. Please describe your company's leasing options, refresh programs, and ability to meet this goal.*

## Verizon Response

Verizon has read and understands.

The following are the certified endpoints that meet or exceed the FedRamp encryption requirements (TLS1.2).

Verizon also understands the need to ensure that the CPE is provided as part of the monthly service and will be supported (break/fix) for the service term.

Since CPE will have a transfer of ownership at the end of the service term, a refresh program will need to be re-negotiated at the end of the service term.

Verizon proposes the following phones for each requirement:

- 2-line phone – Cisco 7821
- 5-line phone with sidecar capabilities – Cisco 8851
- Conference phone – Cisco 7832
- Softphone – Cisco Jabber
- Wireless phone – Cisco 8821
- ADA-compliant phone – Cisco 7821

The Cisco 7821 meets ADA requirements by being hearing aid compatible, meeting FCC loudness requirements and the dialpad is ADA compliant. Section 508 loudness requirements can be met with the use of industry-standard inline handset amplifiers.

## Certified Endpoints

| | |
|---|---|
| Cisco Jabber<br> | Cisco Jabber is the Cisco unified communications client application for Windows PC, Mac OS, iPhone, iPad, and Android that provides presence, instant messaging, voice, HD video, voice messaging, desktop sharing, and conferencing. |
| Cisco IP Phone 8800 Series<br> | The Cisco IP 8800 Series is ideal for a variety of workers and settings throughout your organization. It delivers easy-to-use, highly secure, encrypted, high-quality wideband audio communications, with select models also supporting affordable entry to 720p HD video. In addition, Cisco Intelligent Proximity can integrate telephony features with your personal mobile devices.<br>**Note:** The 8821 phone is not supported with Verizon Federal UCCaaS. |
| Cisco IP Phone 7800 Series<br> | Combines an attractive ergonomic design with always-on reliability, secure encrypted voice communications, and ecofriendly low-power consumption. Delivers advanced IP telephony features and crystal-clear, wideband audio performance to deliver an easy-to-use, full-featured voice communications experience. |
| Cisco DX Series<br> | Quality Collaboration for Every Desk:<br>Work with anyone, anywhere in the world. See and hear each other as if you're in the same room, with the DX Series for your desktop.<br>Simplify your work day, and form real connections with the people you work with, wherever they are. It's collaboration fit for a CEO, but priced for everyone.<br>Note: Availability is expected in CY2017 |

Verizon also requires Certified Routers and Analog Gateways that meet/exceed the FedRamp requirements.

Below are the recommended parts that meet the FedRamp Moderate Standards.

- HCS-G supports VG3xx and ISR4K

Per the State's response in the "Q&A" within Addendum 3, Verizon understands that these items are the State's responsibility.

*4.2.1.1.3.3 The State utilizes Cisco SRST and local voice services in case of data network failure. At the initial deployment of the site to the Vendor's hosted solution, if requested, the Vendor should work with an Agency to implement call control and PSTN connectivity, in case the data network fails at a State location. This should include the provisioning of at least one local phone line for 911 calling.*

*The Vendor should include the provisioning of one failover line in the cost of its monthly package. If the site requests more than one failover line, the State understands there may be additional charges for that work.*

*Please describe your solution's ability to meet this goal and any additional costs.*

## Verizon Response

Verizon has read and understands.

Based on the requirements, Verizon will work with the end users to understand the needs for local SRST and document the design requirements accordingly.

The assumption is that 130 locations using our Standard Security Hosted Voice or 130 locations using our High Security Hosted Voice, will need SRST capabilities.

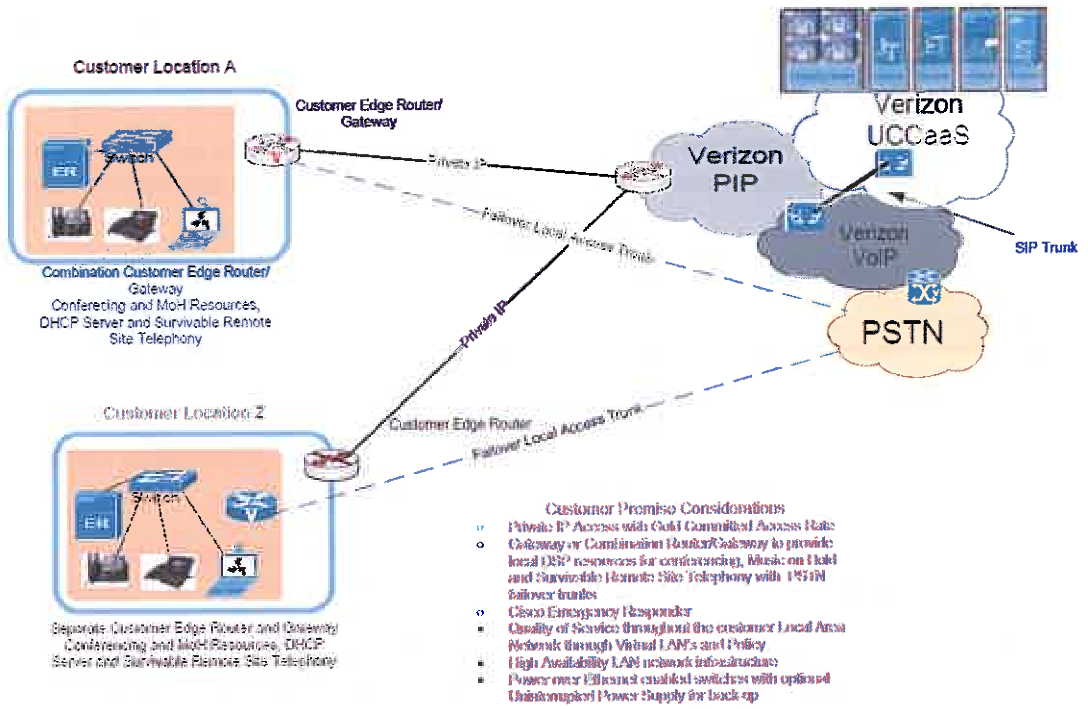
Verizon will not be providing any 1 mbs or ISDN PRIs with our UCCaaS solution. If during discovery that it is identified that more than 130 locations (per Appendix A, revised 10-24-18) need SRST services, additional cost may apply.

*4.2.1.1.3.4 The Vendor's solution should support station-to-station calling that remains "on-net" (on the State's private data network) at no additional cost. Please describe your solution's ability to meet this goal.*

## Verizon Response

Verizon has read and understands.

Station to Station calling is supported when the traffic is routed over the States MPLS network. Here is a sample design using 2 SIP Trunks that connect not only to UCCaaS but also to the PSTN gateways.


Customer Location A
Customer Edge Router/
Gateway
Switch
ER
Private IP
Failover Local Access Trunk
Combination Customer Edge Router/
Gateway
Conferecting and MoH Resources,
DHCP Server and Survivable Remote
Site Telephony
Private IP
Verizon
PIP
Verizon
UCCaaS
Verizon
VoIP
SIP Trunk
PSTN
Customer Location Z
Customer Edge Router
Failover Local Access Trunk
Switch
ER
Separate Customer Edge Router and Gateway
Conferencing and MoH Resources, DHCP
Server and Survivable Remote Site Telephony

Customer Promise Considerations

- Private IP Access with Gold Committed Access Rate
- Gateway or Combination Router/Gateway to provide local DSP resources for conferencing, Music on Hold and Survivable Remote Site Telephony with PSTN failover trunks
- Cisco Emergency Responder
- Quality of Service throughout the customer Local Area Network through Virtual LAN's and Policy
- High Availability LAN network infrastructure
- Power over Ethernet enabled switches with optional Uninterrupted Power Supply for back up

*4.2.1.1.3.5 The Vendor's solution should provide at least two PSTN connections via SIP Trunks over secure private connections engineered for voice quality of service.*

*These PSTN connections should adhere to the industry standard of 150 mis latency or better, and jitter of 40 mis or better. Please describe your network engineering architecture and your practices to continuously achieve these standards.*

## Verizon Response

Each Hosted Voice data center has two separate secure connections to Verizon Session Border Controller (SBCs) nodes located is geographically diverse cities. Inside each SBC node, the SBCs are deployed as HA pairs.

The connections between the data centers and SBC nodes are engineered for voice and are monitored to ensure proper operation. The SBC nodes are connected to multiple geographically diverse voice gateways that connect to the PSTN.

Connections from the State of West Virginia to the Hosted Voice data centers use either Verizon's Private IP MPLS service or secure connections for Mobile and Remote Access users via Expressway C and E servers located in each Hosted Voice data center.

Verizon complies with the industry standard 150 ms latency and 40 ms jitter. Further, Verizon uses a Mean Opinion Score (MOS) metric as calculated using the standards-based E-model (ITU-T G.107) to measure overall call quality.

The E-model takes into account a wide range of telephony-band impairments including delay, jitter, loss, noise, codec conversion, and echo.

Verizon's VoIP SLA includes the following metrics:

- Jitter – 1 ms
- Mean Opinion Score – 4.0
- Network Availability – 99.99%
- Time to Repair – 4 hours
- VoIP Provisioning Interval – 20 calendar days from time a clean order is submitted to Verizon's provisioning group

*4.2.1.1.3.6 The Vendor's solution should provide a MPLS network connection to Verizon' s MPLS core to reduce and/or eliminate the backhaul of traffic to the State's core network. The State has provided a column on the Pricing Page for both one-time installation costs and for monthly recurring costs for these connections. Please describe your ability to meet this goal.*

## Verizon Response

Verizon has read and understands.

Verizon is the current provider of the MPLS network for the State of West Virginia.

*4.2.1.1.3.7 As an option for small sites with non-private network handoffs, the State desires a solution utilizing public networking with the ability to securely transmit sensitive data. Please describe any offerings to support this goal.*

## Verizon Response

Verizon has read and understands.

Verizon is providing two options to connect using non-private networks – one using Verizon Virtual Communications Express and one using Cisco Expressway. Virtual Communications Express pricing is shown on the Cost Sheet as the Small Site Option, per end-user.

With Virtual Communications Express (VCE), you get end-to-end communications delivered from our cloud. You get phone service that is packed full of features that can help make your business more efficient and productive.

Verizon can provide a selection of state-of-the art phones, instant messaging and presence, audio and video conferencing, and desktop and mobile screen sharing that will enable you to collaborate internally and with your customers and suppliers better than ever before.

### Enterprise-Level Power, Functionality, and Features

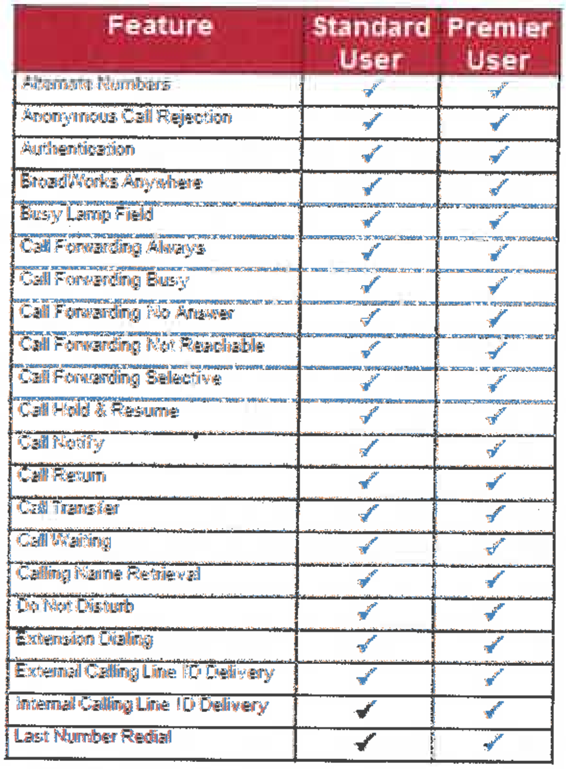
Virtual Communications Express (VCE) is a robust, yet simple "plug and play" or professionally installed solution.

- Benefits and efficiencies of anytime unified communications capabilities across corporate voice and IT systems.
- Ability to boost productivity using existing broadband Internet service or Private IP connections.

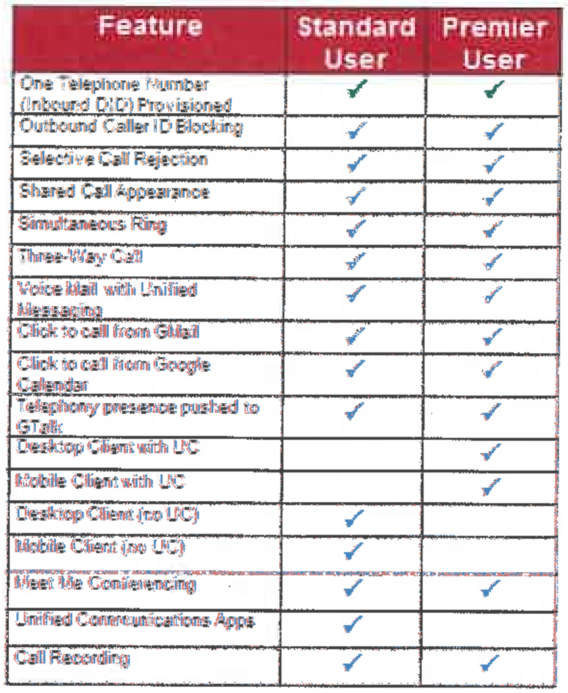
  The State of West Virginia can use the collaborative and mobile tools that VCE offers – i.e. audio and video conferencing – to easily and quickly bring employees or clients together when making decisions.

  Mobile clients can also enable the ability to take calls and conduct conference meetings while on the go. You can remain productive when outside of the office (unlike plain old telephone service), and maintain continuity, so your business can continue to run smoothly.
- Alleviate the effort, complexity, and risk associated with technology management.
- Access leading applications and self-service capabilities.
- Simple installation and activation – no IT expertise required.
- Seamless communication across your organization, right "out of the box" or an optional

## User Features



| Feature | Standard User | Premier User |
|---|---|---|
| Alternate Numbers | ✓ | ✓ |
| Anonymous Call Rejection | ✓ | ✓ |
| Authentication | ✓ | ✓ |
| BroadWorks Anywhere | ✓ | ✓ |
| Busy Lamp Field | ✓ | ✓ |
| Call Forwarding Always | ✓ | ✓ |
| Call Forwarding Busy | ✓ | ✓ |
| Call Forwarding No Answer | ✓ | ✓ |
| Call Forwarding Not Reachable | ✓ | ✓ |
| Call Forwarding Selective | ✓ | ✓ |
| Call Hold & Resume | ✓ | ✓ |
| Call Notify | ✓ | ✓ |
| Call Return | ✓ | ✓ |
| Call Transfer | ✓ | ✓ |
| Call Waiting | ✓ | ✓ |
| Calling Name Retrieval | ✓ | ✓ |
| Do Not Disturb | ✓ | ✓ |
| Extension Dialing | ✓ | ✓ |
| External Calling Line ID Delivery | ✓ | ✓ |
| Internal Calling Line ID Delivery | ✔ | ✓ |
| Last Number Redial | ✔ | ✓ |



| Feature | Standard User | Premier User |
|---|---|---|
| One Telephone Number (Inbound DID) Provisioned | ✔ | ✔ |
| Outbound Caller ID Blocking | ✓ | ✓ |
| Selective Call Rejection | ✓ | ✓ |
| Shared Call Appearance | ✓ | ✓ |
| Simultaneous Ring | ✓ | ✓ |
| Three-Way Call | ✓ | ✓ |
| Voice Mail with Unified Messaging | ✓ | ✓ |
| Click to call from GMail | ✓ | ✓ |
| Click to call from Google Calendar | ✓ | ✓ |
| Telephony presence pushed to GTalk | ✓ | ✓ |
| Desktop Client with UC | | ✓ |
| Mobile Client with UC | | ✓ |
| Desktop Client (no UC) | ✓ | |
| Mobile Client (no UC) | ✓ | |
| Meet Me Conferencing | ✓ | ✓ |
| Unified Communications Apps | ✓ | |
| Call Recording | ✓ | ✓ |

✔ = Included
✓ = Optional

## The VCE Solution

VCE is a robust, resilient hosted solution for your business offering simple, scalable IP Voice with enterprise-grade power and functionality, such as Unified Communications, inbound eFax, mobile/desktop clients, business continuity, auto-attendant, and hunt groups.

VCE supports Verizon Certified IP handsets with an optional feature to support Android and Apple smartphones with a mobile client to allow single number reach. If the feature is required upon discovery, additional costs may apply. This means you can be reached via one phone number, whether in the office at your desk or on your mobile phone.

VCE can be delivered over Verizon Private IP, Internet access or any 3rd party Internet access. VCE is Competitive, predictable, flat monthly price per user, which includes the DID, call control features, voicemail, and enterprise-grade features, such as music on-hold, hunt group, auto attendant and call queuing.

Phones can be purchased or rented (they are not included in the per user price).Limited or no capital investment required.

VCE is able to scale up or down for growth or seasonal variation with rapid deployment capability to provide the ability for The State of West Virginia to bring on new sites quickly and efficiently. The online management portal enables administration of user accounts.

### Cisco Expressway

Select Cisco phones and the Jabber client can connect to the Hosted Voice data centers using Cisco Expressway. Expressway provides secure, encrypted session-based access for remote and mobile workers, without the need for a separate VPN client.

Secure firewall traversal technology that enables unbounded mobile use cases: Cisco Expressway for Mobile and Remote Access enables users to easily access their Jabber collaboration services outside the corporate network, allowing them to be more productive when they are mobile.

In contrast to VPN, it secures only Jabber traffic, helping ensure that the user's personal data does not cross the corporate network. Most new Cisco phone models can also use Expressway natively allowing a small office to use commercial Internet access from any provider as the access method to reach the Hosted Voice data centers.

Devices may also leverage Verizon Wireless Private Network in combination with UCCaaS to ensure mobile devices are always connected to the enterprise. This feature is referred to as UCCaaS Mobile First Private Network.

For additional information, please reference the Virtual Communications Express Overview provided in Appendix H of this proposal.

*4.2.1.1.3.8 The Vendor's solution should include Caller ID services (inbound traffic) and custom number and naming (outbound traffic) that State Agencies may utilize to customize their displayed information. The Vendor should provide this capability at no additional cost. Please describe your solution's ability to provide these services.*

## Verizon Response

### Caller ID with Name (Inbound)

Verizon provides the VoIP subscriber the name of the calling party. If name is not available, city/state will be populated.

### Caller ID Name and Number (Outbound)

Verizon supports outbound custom telephone number through Alternate Caller ID. This custom number will be sent to the terminating provider. Verizon also supports outbound custom Caller ID with Name (CNAM).

The custom name must meet the PSTN CNAM Database standards (maximum length, allowable words, etc.). However, CNAM is a function of the receiving end's provider.

Verizon provides the custom name to the various third party database providers. It is up to the terminating provider to update their databases with the custom name.

*4.2.1.1.3.9 The Vendor's solution should include unlimited local and nationwide calling at no additional charge. Please describe your no cost offerings.*

### Verizon Response

Verizon has read and understand.

Verizon will be providing unlimited local and domestic long distance service. The price is included in the based rate per concurrent call.

*4.2.1.1.3.10 The Vendor's solution should provide international calling. The State understands fees may be associated with international calling. The Vendor should provide the per minute international calling rates for Mexico, Canada, and Jamaica.*

*The Vendor should also attach an appendix of international calling rates for all countries. The State will allow for quarterly Change Orders to updates these international rates. Please describe your solution's international calling offerings.*

### Verizon Response

Verizon has read and understood, and has provided the 3 countries requested on the VOIP

International calling rates located within the price sheet in the cost proposal. See Appendix A in the cost proposal for all other International calling rates.

*4.2.1.1.3.11 The Vendor's solution should provide comprehensive site coverage to meet the State's local and long-distance IP-based calling requirements. Please describe your coverage, as well as how you plan to meet the State's coverage needs.*

### Verizon Response

Verizon has read and understand.

Verizon will be providing unlimited local and domestic long distance service. The price will be based on the number of concurrent calls. Verizon's VOIP availability (percent of businesses served (in terms of businesses with 20+ employees) is 80.1% in the State of West Virginia.

Verizon meets this requirement by providing local VoIP DID numbers in the State of West Virginia. Based on the locations listed in Appendix A, Verizon serves all but fifteen of these locations currently.

For locations in an area not served by local Verizon VoIP today, PSTN connectivity will be provided via the local router and local PRI/Centrex/POTS service provided by the current State of West Virginia contract holder of those services.

Upon contract award, Verizon will evaluate these locations for expansion of local VoIP service. If expansion makes business sense, these sites will be converted to Verizon VoIP once local VoIP is available.

Verizon is continually updating its VOIP availability on a weekly basis nationally.

*4.2.1.1.3.12 The Vendor's solution should provide load balancing for all traffic in-bound from the PSTN. Please describe your solution's ability to meet this goal.*

## Verizon Response

Verizon has read and understands.

The VOIP design can meet inbound from the PSTN load balancing.

*4.2.1.1.3.13 The Vendor's solution should ensure 911 call delivery to the appropriate local PSAPS. Additionally, the State desires support for Private Switch/Automatic Location Identification (PS/ALI) services for 911 calls. Please describe your process for ensuring the accuracy of 911 call delivery, as well as the process to support PS/ALI.*

## Verizon Response

Verizon has read and understands.

Verizon's UCCaaS service supports direct (911) and indirect (9 911) dialing of emergency services. Customers that require accurate emergency call location identification can use the Cisco Unified Communications Manager Native Emergency Call Routing feature.

The DIDs for each location will be assigned to that location's address. Any calls to 911 from that DID will be routed to the proper PSAP based on the location address.

If more detailed location information is needed (e.g., room, floor or building), detailed location information can be added to each number in the online Integrated Administrative Console (IAC) portal by the State of West Virginia.

While this can be done manually for each DID, any moves have to be manually updated. Cisco Emergency Responder (CER) provides a better solution by assigning Emergency Location Identification Numbers (ELINs) with associated Emergency Response Locations (ERLs) to each area.

With CER, only the ELINs would need to have their detailed information location entered in the IAC. This will allow individual phones to be moved without having to manually update the location information in the IAC for that DID. CER is available as an optional service for Hosted Voice for an additional charge per user.

PS/ALI is also supported. This can be provided by Verizon with a partnership with RedSky. Pricing for this service would be provided after discovery has determined the specific requirements.

*4.2.1.1.3.14 The Vendor's solution should support the following industry standard protocols: G.711 (uncompressed), G.729 (compression), and T.38 (fax). Please describe the protocols supported by your solution.*

## Verizon Response

Verizon has read and understands. Verizon VOIP supports G.711, G.729 and T.38 codecs.

*4.2.1.1.3.15 The Vendor's solution should have the ability to scale the number of simultaneous concurrent calls on a monthly and/or seasonal basis at the State's request. Please describe your solution's ability and your process to accomplish this, including division of duties.*

## Verizon Response

Verizon has read and understands.

The concurrent call count can be throttled up or down on demand via the Verizon Enterprise Center portal by the State of West Virginia VOIP administrator/administrators.

*4.2.1.1.3.16 The Vendor's solution should include interoperability with the following: IPv4 addressing (RFC 791), RFC 1918 for private IP addressing, and support SIP over TCP or UDP.*

*Carrier grade NAT (RFC 6598), link-local IP addresses (RFC 3927), and Multicast addresses (RFC 3171) will not be accepted. Please describe your solution's interoperability to accomplish this goal.*

## Verizon Response

Verizon has read and understands, but with clarification.

Verizon supports SIP over UDP only.

*4.2.1.1.3.17 The Vendor's solution should provide the following quality and reliability standards: QoS tagging IEEE 802.IQ-2011; not rewriting, marking, or remarking any VLAN tags affixed to packets by the State, without the State's expressed consent; at a minimum, one Class of Service (COS) marking per Ethernet service.*

*Please describe your solution's ability to meet this goal.*

## Verizon Response

Verizon has read, understood and complies.

Verizon's Private IP MPLS service provides six classes of service to include:

- EF
- AF4
- AF3
- AF2
- AF1
- BE

*4.2.1.1.3.18 The State desires a Unified Messaging solution; therefore, the Vendor's solution should fully integrate with Microsoft 0365, allowing users to listen, forward, and delete voicemails from both 0365 and the hosted environment.*

*Voicemails should be retained in the solution for 15 days or longer. In addition, the Vendor's solution should be provisioned to fully integrate with the State's Active Directory and Active Directory Federated Services. Please describe your abilities to meet these goals.*

## Verizon Response

Verizon has read and understands.

Verizon supports single inbox integration with Microsoft O365 to allow users to listen, forward and delete voicemails from both O365 and the hosted environment. A user may retain voicemail messages for as long as they like subject to standard maximum mailbox size of 14 MB (approximately 29 minutes).

Verizon will integrate with the State of West Virginia's Active Directory and Active Directory Federation Services.

*4.2.1.1.3.19 Some State Agencies utilize paging and notification to the PC desktop, over-head paging, or through-the-phone- speaker paging. The Vendor's solution should include an option for providing, maintaining, and supporting a paging solution, including any associated hardware, software, and licenses, and if requested by Agency, or integrate with an existing or Agency-owned paging solution.*

*The State understands there may be fees associated with this offering. Please describe your offerings with respect to these deployments.*

## Verizon Response

All Paging Service pricing is completed on an Individual Case Basis (ICB) after an assessment has been completed.

The paging systems are unique in nature and priced based upon site conditions; scope/scale and specific requirements not represented in this RFP and are to be determined upon discovery sessions by the State of West Virginia and Verizon.

Verizon has included in our response hourly rates for Paging Integration for the following positions as required in the RFP Attachment A, Cost Sheet:

- Project Manager
- Network Engineer
- Telephony Engineer

Verizon can offer paging services to the State of West Virginia utilizing the Professional Services engagements as listed in the RFP cost sheet for Custom Implementation Services and Fees and a custom Scope of Work and bill of materials representing fees associated with this offering.

Paging Services can be implemented in the following approaches:

1) Verizon can provide software based paging service, which integrates with our Verizon UCCaaS platform, such as Singlewire InformaCast. This solution could be installed in the State of West Virginia OOT Data Center or at a particular Agency location as directed by the State of West Virginia.

2) Verizon can provide hardware based paging system which operates as a stand-alone appliance. This solution could be installed at a particular Agency location as directed by the State of West Virginia.

3) Verizon can provide maintenance/repair/MAC services on the Agency-Owned hardware based paging system which operates as a stand-alone appliance.

*4.2.1.1.3.20 The State desires an option for Agencies with high call volume and receptionist personnel that will utilize an Operator Console for fast and efficient call control. The State understands there may be fees associated with this offering. Please describe your solution's Operator Console offerings.*

## Verizon Response

Verizon has read and understands. Verizon's UCCaaS solution is able to be integrated with the State of West Virginia's existing Bridge Operator Console for an install charge as long as the State or vendor provides documentation on how to integrate with Cisco HCS.

Verizon does not support any troubleshooting with the Bridge Operator Console. Additionally, Verizon can provide Cisco Unified Attendant Console Standard and Advanced for a monthly charge shown on the Cost Sheet as requested with monthly recurring fee.

Advanced Attendant instance from 1-50 instances can be provided on an individual case basis during discovery, an additional cost may apply.

*4.2.1.1.3.21 If requested by an Agency, the State desires the ability to integrate a third-party call recording solution with the Vendor's hosted solution. Please describe your solution's ability to meet this goal.*

## Verizon Response

Verizon has read and understands.

Verizon is proposing UCCaaS, VCE and the Virtual Contact Center (VCC) solutions. VCC does support call recording for VCC users.

If State of West Virginia Agencies require call recording for Non-VCC users, Verizon can provide optional third-party call recording solution integration for UCCaaS. If required upon discovery and additional costs may apply.

*4.2.1.1.3.22 The State desires that the Vendor use currently-owned State IP telephony handsets where the handset is still supported on the Vendor's solution. Please describe your company's ability to use the State's current handsets and its ability to meet this objective.*

## Verizon Response

Any currently supported Cisco phone (not past the End of Support date) can be used on the standard Hosted Voice platform. Cisco phones that are past the End of Support date may be used on the standard security platform, but they are not supported by Verizon for troubleshooting purposes.

Note that certain phones deprecate with each HCS software release, and these phones will not work once that release is enabled for the State of West Virginia.

Third party phones are allowed on the standard security platform if the State of West Virginia or phone vendor can provide release notes that show how these phones connect with Cisco HCS and are approved by Verizon. These phones are also not supported by Verizon for troubleshooting purposes.

Locations requiring the high security option must use specific phone models that are certified to meet the security requirements of the high security platform. Verizon is proposing new handsets meeting full compliance on the HCS-G platform.

*4.2.1.1.4 Hosted Contact Center Services*

*4.2.1.1.4.1 The State's goal is to obtain a reliable, customizable, and scalable solution to provide hosted contact center services for an estimated twenty-five (25) individual contact center sites that works in conjunction with the Vendor's proposed Hosted VoIP solution.*

*Certain sites require the capability to transmit and/or store call recordings that may contain sensitive data (such as PHI or PII). For ease of deployment and maintenance, the State prefers the contact center solution be web-based.*

*The solution should provide the following capabilities*

- *Ability for a simple, drag-and-drop, easy-to-understand interface to create customized call routing and role- based queues that can be deployed to sites with non- technical administration*
- *Should provide chat capabilities*
- *Should provide live data reporting*
- *If requested by an Agency, the solution should have the ability to interface with an Agency's database to populate information based on data provided by the caller*
- *If requested by an Agency, the solution should provide the flexibility for agents to use a public-switched- telephone-network (PSTN) phone to utilize the solution*
- *Should provide scalability for up to 800 agents and the ability to expand in the future*

*Please describe your solution and identify any areas in your solution that exceed the items requested above.*

## Verizon Response

Verizon has read, understood and will comply.

Verizon's Virtual Contact Center (VCC) is powered by NICE inContact. Together the partnership offers the only complete cloud contact center solution.

NICE inContact is the only provider to be recognized as a leader by all five major CCaaS analyst firms, their software is helping organizations around the world improve their customer experience with a unified suite of Omnichannel routing, workforce optimization and analytics – delivered on an enterprise-grade open cloud platform.

Verizon's VCC NICE inContact built a complete platform that intelligently routes all of your customer interactions, integrates with leading CRMs, and helps you schedule and improve your workforce and analyze trends.

### Proposed Solution

VCC is a purely cloud solution that is highly scalable, and has the ability to provide nearly instantaneous scalability if needed. VCC is presently implemented in several State of West Virginia departments including Tax and DHHR.

VCC will leverage years of expertise to design and implement a contact center solution tailored for you. The feature rich VCC platform will enable you to cost-effectively leverage our award-winning advanced skills-based routing and universal queue to quickly connect customers with the agents skilled to help, on the channels your customers choose to interact.

VCC is designed to support contact center agents outfitted with a dialable phone, a HTML5 browser PC and an internet connection. The agent may be working within a large contact center, a small business or from home. It makes no difference to the functionality that is available. VCC sees all agents the same way, no matter where they are located.

VCC enables agents to log in securely with any HTML 5 based browser. The VCC Agent is a multi-media agent interface which communicates to VCC when the user is available or unavailable, and allows the agent to execute various tasks such as answering contacts, transferring contacts, putting contacts on hold, conferencing, managing emails, chats, SMS (optional), voicemail and work items.

VCC works with Verizon IP Toll Free and/or VOIP Inbound Local Origination (VILO). If upon discovery is required additional charges will apply.

By having a solution integrating the telecom and contact center assures increased performance, simplifies troubleshooting, and reduces cost. Network connectivity into and out of the VCC platform do not incur additional charges and LD charges out of the platform are suppressed.

In summary, we combine the best contact center solution with our deep experience in telecommunications, empowering each of our customers to improve agent productivity, customer service quality, and operational efficiency.

Given the States Response to questions in Addendum 2 & 3 where the response includes that "discovery is a part of the RFP" related to optional hosted Contact Center features, Verizon will undertake discovery upon award and those items not disclosed by the State will be evaluated for effort and potential modifications to pricing may be required to add the services identified.

### Cloud Contact Center Platform

VCC assists agencies respond to incoming inquires whether from phone, email, web, chat, or text. VCC is an award-winning cloud solution that doesn't require expensive hardware or software.

Start with ACD and IVR, the building blocks of our platform, and if upon discovery, optional features such as customer feedback, CRM/ CTI integration, dialers, quality management, workforce optimization and management, custom reporting and analytics are required, additional charges may apply.

The advanced skills-based ACD software quickly matches callers in the queue to the agents who can best assist them. That means efficient call resolution, customer satisfaction, and potential operational savings from a multi-channel contact center.

The ACD system is the core of the VCC platform – all routing solutions require automatic call distribution and build upon this functionality.

### Interactive Voice Response

The IVR system can reduce costs per call by letting callers choose the type of help they want such as self-service (if self service is required during discovery, additional non recurring costs may apply) or speaking to an agent.

Not only will the IVR solution potentially free up resources to handle more complex cases, but customers can quickly self-solve basic issues specific to the contact center contacted.

### Agent Interface

VCC's agent interface, MAX (My Agent eXperience - MAX), is fully HTML5 context-sensitive interface designed for the streamlined handling of all contact center interactions across all media channels. With MAX, agents will be ready to handle incoming contacts and complex interactions while focusing on positive customer experience.

A Unique Logged in Agent who logs into to the ACD / Dialer platform at any point, for any duration, during the billing interval will include the following:

- 1 ACD Agent
- 1 Campaign Dialer Agent (For a selected station, the agent can operate either as an ACD agent or as a dialer agent at any given time. Initial availability of campaign dialing functionality requires an optional Dialer Implementation.)
- 1 Universal Port – Used for IVR and voice, but does not affect chat or email
- 1 GB Data Storage and Management for storage of recordings, prompts, scripts, messages, files, and more.
- Includes access to call monitoring and call conferencing
- Accounts support FTP or SFTP delivery of basic call recordings
- Supervisor reporting
- ACD / IVR programming toolset (i.e., VCC Studio)

### Studio

VCC Studio is a powerful rapid application development tool providing the State with access to everything needed to create and maintain Omni-channel routing strategies and queue processing flows from a single interface.

From optional Application Program Interface (API) integration to many predefined routing actions – Studio is the visual, intuitive interface to ensure every contact is treated and routed exactly as desired, easily creating the customer experience for each department's needs.

Every component of the VCC solution can be managed remotely since it is a cloud-based solution

### Central

VCC Central is a browser-based secure interface for handling administrative and reporting tasks on the platform.

Administrators have the ability to perform tasks with ease, such as: view real-time reporting, set up security profiles and user accounts, create multi-channel skill or queue groups, assign hours of operations conditions, as well as define the routing behavior of the ACD. It is the "Central" administrative interface of the Platform.

Every component of the VCC solution can be managed remotely since it is a cloud-based solution

### Analytics & Reporting

Contact Center Analytics & Reporting is a flexible, easy to use feature that lets contact center supervisors, managers, and administrators track critical metrics so they can make smart operational decisions.

Real-time reporting includes pre-built reports, ad-hoc reporting, or the ability to create your custom templates. Closely track real-time management metrics with a customizable dashboards for full reporting customization

### Hardware/Software (State of West Virginia provided)

To facilitate a good VCC user experience, each agent needs a computer with mouse, keyboard, and color monitor. In addition, the minimum workstation requirements are listed below.

### Computer Operating System

- Windows 7 & 8 32/64 bit
- Windows 10

### Computer Speed

- Intel i3 processor or higher at 3GHz or better. If using Personal Connection dialer at dialing ratio higher than 3:1, a faster CPU and additional RAM is recommended
- 1GB RAM or more

### Screen Resolution

1024 x 768 or above for improved user experience

### Supported Browsers

- Internet Explorer 11
- Google Chrome
- Safari
- Firefox
- MS Edge

### Browser Configuration & Add-ons

- Cookies Enabled
- Popups Enabled
- JavaScript Enabled

- Adobe Shockwave Flash Player 9 or above
- Java Applets Enabled with Java Virtual Machine 6.11 or above installed
- Windows Media Player Plugin

### Internet Broadband Access Required:

- 35 kbps bandwidth per PC workstation
- Less than 200ms average round-trip ping reply between workstation and NICE inContact servers

### VoIP Bandwidth Requirements

- Based on the CODEC implementation
- 711 CODEC requires 88 kbps per simultaneous calls
- 729 CODEC requires 40 kbps per simultaneous calls

(For example number of simultaneous calls x CODEC kbps = total bandwidth needed)

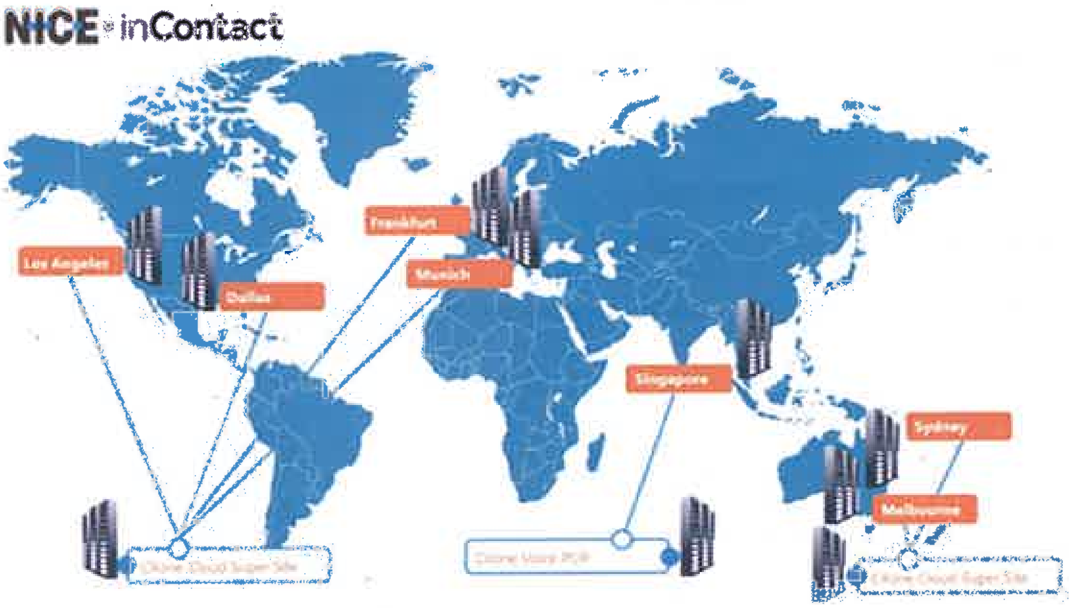
CODEC bandwidth use is bi-directional, so it is 88 up and 88 down simultaneously for a given G.711 call.

### Architecture

Fully redundant and protected power is critical to today's data centers. VCC data centers are Active/Active to improve Business Continuity and operate with the most advanced equipment available to ensure that you receive the best technology possible without having to purchase it on your own.

The following network diagram provides a simplistic picture of NICE inContact's network and redundancy.

NICE inContact has six fully redundant Active/Active cloud super-sites: two in North America; two in Europe and two in Australia.



The sites are supported and monitored by a 24/7 carrier-grade Network Operations Center (NOC) located at our corporate offices in Salt Lake City and a redundant NOC site in California.

The NOC employs next generation, carrier grade, industry-standard monitoring systems and tools and, in the event of failure, has the ability to operate remotely utilizing NICE inContact technology either within Salt Lake City or Los Angeles.

Verizon network in support of VCC provided at NICE inContact data centers is designed for redundancy and failover. The core IP network is connected via a dual SONET ring backbone, meaning two redundant fiber links.

Along with redundant edge routers, core routers, firewalls and VoIP hardware, multiple ISP and diverse toll-free carriers, our network infrastructure provides reliable, stable, service-rich benefits.

This broad range of connectivity models and solutions allows for the highest level of selection in hosted IP telephony and call center applications. Each server center functions as both a primary location, and as a backup to the other server center in the event of a problem.

If a major outage were to take place in one data center, for instance, the next call would be completed through the second server center. All historical data, call flows and other information would continue uninterrupted.

The network operating centers function with 24/7 on-site and biometric securities. Through the IP backbone, our networking infrastructure connects our sites via bandwidth pipes that can be routed through a private connection. We also have state-of-the-art intrusion detection systems in place to keep our system safe from hackers.

NICE inContact utilizes redundant equipment, facilities, connections, power supplies, cooling systems and databases to ensure that your contact center is always up and running smoothly and assure the 99.99% availability SLA is met.

### Optional Solutions

VCC is a full featured solution. Some contact centers in West Virginia may require features beyond the mandatory requirements.

If during discovery, it was determined there was a requirement beyond the mandatory requirements, a sample of the suite of solutions below can be used to meet those requirements. Additional charges may apply for these features

### Outbound Solution

With our outbound dialer, callers will never hear a delay again. This outbound solution eliminates awkward delays when greeting a caller, while increasing productivity, conversion rates, and revenue as agents make multiple predictive calls.

The optional outbound solution enables compliance with Do Not Call List Management and Intelligent Call Suppression, blending of inbound and outbound agents, as well as the ability to synchronize with external systems with integration. Outbound can be via call, SMS or e-mail

### CRM Integrated Solutions

NICE inContact CRM integration helps agents personalize calls using CTI screen pops and more. Identify callers by unique attributes, like phone number, and display information, such as the caller's name, on the agent's screen before the call connects. We can integrate with major CRMs, as well as with most custom CRMs.

### Workforce Optimization (WFO)

VCC Workforce Optimization (WFO) empowers our customers with new visibility into the customer experience so you can track KPIs, reach goals, and fix what's not working.

WFO also enables our customers to analyze customer interactions with Quality Management, use call data to create schedules via Workforce management and enhance visibility, use Workforce Optimization Software to target and improve Key Performance Indicators (KPIs), discover the root cause of customer and employee behavior, as well as address skill deficiencies and ensure consistent coaching across your organization.

### Quality Management (QM)

Monitor agents' performance and give them helpful coaching and training with Quality Management solution. Capture multi-media customer interactions and quickly score them against pre-defined criteria using our flexible and customizable evaluation forms. Improve employee performance with personalized coaching sessions.

### Workforce Management (WFM)

Most contact volumes aren't static all day—why should staffing levels be? WFM enables achievement in balance of employee needs, customer satisfaction, and cost containment by ensuring the right agents with the right skills are available at the right time.

By matching customer demand to your scheduled workforce, VCC's call center workforce management system assists you in creating the best-case staffing scenario, and ensuring adherence with real-time visibility into staffing and call volumes.

### Customer Satisfaction Surveys

VCC Customer Survey Solutions ensure high customer satisfaction by gathering callers' feedback immediately after calls end with survey results.

Gather real-time comments with customer satisfaction surveys while the call is still fresh in the customer's mind and get invaluable information about your agents' performance and your processes.

Use reports that summarize and analyze critical customer feedback to coach and give kudos to agents, accurately measure customer retention, and pinpoint additional areas for improvement.

### inView Real-time Dashboards

inView is a real-time performance management tool developed to meet the specific needs of front line sales and service activities.

inView increases efficiency for management, supervisors, and agents by delivering real-time, personalized performance data and business intelligence to every employee on the floor while automating critical managerial activities.

inView is a revolutionary, optimization solution engineered by call centers for call centers that drives successful execution by aggregating performance data from disparate systems and acting on the data with proven business improvement processes.

inView increases accountability and creates a culture of continuous development essential to reaching business objectives.

### Speech Analytics

Omnichannel Analytics is an intelligent linguistic analytics engine that converts contact center calls, email, and chat transcripts into consumable data that allows contact center supervisors and managers to better understand what is happening in the contact center. The application parses and categorizes contact data, and clarifies it based on context.

Automate your approach to call recordings, identify customer concerns through speech detection, and identify opportunities for improvement in business processes, experience, and performance.

VCC enables efficient recording processes with quantifiable data and enhance visibility into compliance by bringing analytics into your contact center.

### Workforce-Intelligent Contact Center (WFI)

Workforce- Intelligent Contact Center (WFI) eliminates manual interventions and inefficient processes by integrating contact center infrastructure and Workforce Optimization (WFO) systems.

WFO performance data can now drive ACD and IVR behavior, so your team spends less time manually checking agent performance and adjusting assignments, while we automatically optimize the customer experience based on many measurements and adjustments. The result is an improved customer experience, high productivity, and operational efficiency.

*4.2.1.1.4.2 Some of.the State's call centers operate on a 24x7x365 basis, delivering critical services to the communities.*

*As such, the State prefers the Vendor's solution have inherent redundancy and survivability characteristics that will ensure minimal service disruptions, such as data centers in geographically diverse regions allowing for failover, equipment and power redundancies in those data centers, etc.*

*Please describe your solution's redundancy and its ability to meet and/or exceed this goal.*

### Verizon Response

The VCC platform runs in an Active/Active configuration and is designed for seamless redundancy and failover. The core IP network is connected via a dual SONET ring backbone, (IE. two redundant fiber links).

Along with redundant edge routers, core routers, firewalls and VoIP hardware, multiple ISP and diverse toll-free carriers, our network infrastructure provides reliable, stable, service-rich benefits.

Geographically diverse data centers (LA and DALLAS), EMEA (Frankfurt and Munich), and Australia (Melbourne and Sydney) High availability design applied to carriers, networks, hardware and applications.

Internally NICE inContact uses sophisticated replication, database mirroring, and ETL processing to maintain two synchronized copies of its databases in geographically separated data centers.

The databases are configured Active - Active and intelligent health checks are used to transparently move database access should a failure occur.

*4.2.1.1.4.3 The Vendor's solution should include enhanced features for Administrators, Supervisors, and Agents to effectively meet the needs of their customers. As such, the solution should provide the following capabilities:*

- *Agent and Supervisor client that provides Blended agents: Inbound and outbound capability*
- *Ability to monitor critical performance metrics allowing managers to coach, train, and encourage agent behavior*
- *Ability for Supervisors to change an agent's status*
- *Ability for Supervisors to silently monitor inbound and outbound calls*
- *Ability to interrupt an agent's call to interact with both the caller and the agent*
- *Ability for Supervisors to remove an agent from a call*
- *Ability to change an agent's skill profile in real time Please describe your solution and identify any areas in your solution that exceed the items requested above.*

## Verizon Response

VCC is a true Omnichannel Session Handling (OSH) system that allows agents to actively work on multiple contacts across multiple channels at the same time if required.

This is different from how concurrent chats and emails are handled in Single-Channel Handling because of how the contact time is managed and how agents are able to handle contacts across any channels at the same time.

As an example, agents can be on a phone call while handling two chats and three emails, all concurrently.

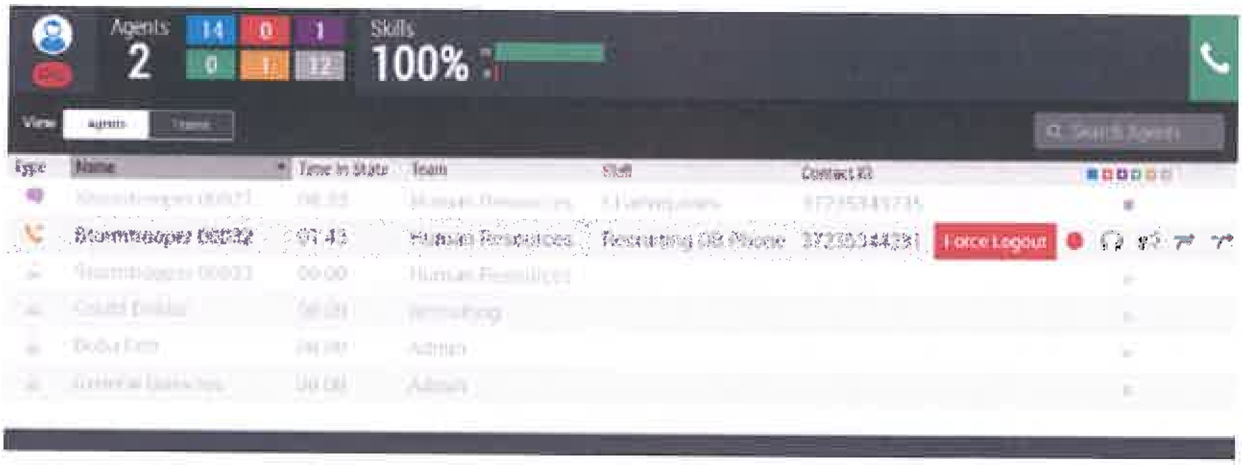
This information is all captured and reportable. We can provide detailed analytics that can then be stored or memorialized in your specified databases or CRMs (if required during discovery additional NRCs would apply).

Multichannel information and contact details can be utilized in multiple reports and graphs to best represent the performance metrics of the organization.

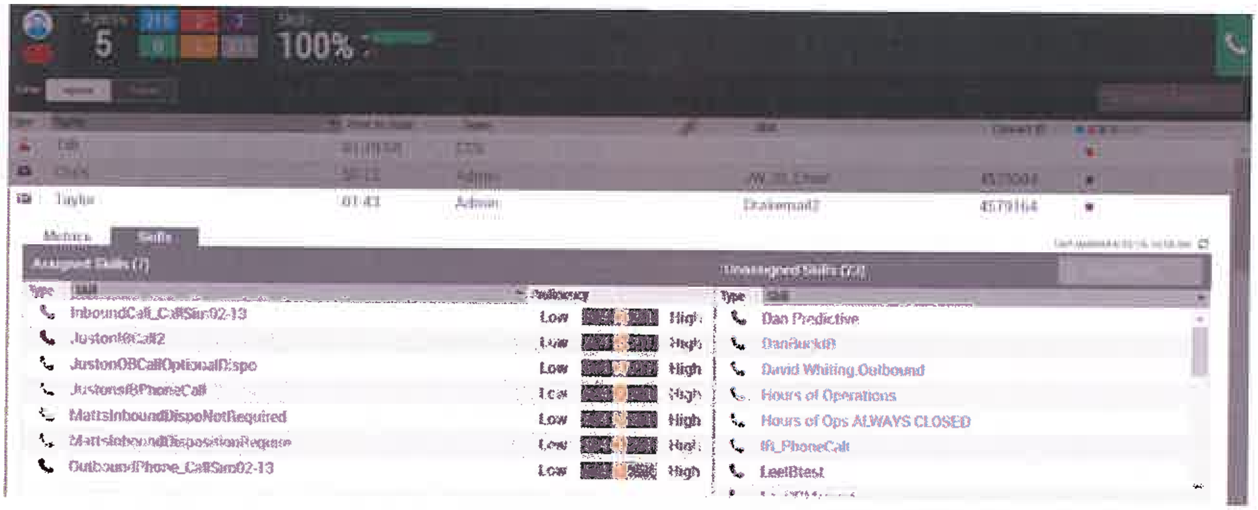
The VCC Supervisor interface allows you to perform critical daily job functions, such as monitoring and interacting with agents, while maintaining a real-time pulse on contact center performance.

You can discreetly listen to calls, coach agents on calls without the contact hearing you, barge in on calls so both the agent and the contact can hear you, take over calls to disconnect the agent and manage the rest of the call yourself, and force an agent to log out of the Agent application.

The following shows the Supervisor interface. You can see next to the highlighted agent the ability to Force Logout, Listen to, Whisper coach, Barge or Take-over a voice interaction.



Also under the Supervisor interface you can adjust agent skills and proficiencies in real-time. Below is an image of how supervisors can click to add skills to specific agents:



*4.2.1.1.4.4 Some State agencies require the ability to utilize call recording, both on-demand and session-initiated.*

*Certain call recordings will contain sensitive data (PHI, PII, etc.) and will require proper security protocols when transmitting or storing this information, with role-based access as defined by the State.*

*Please describe your solution's call recording capabilities, and any additional requirements for the State in order to utilize these features.*

## Verizon Response

Recording of calls is a function of the platform, and can be controlled by an Interactive Voice Response (IVR) script, or started by a manager or agent (depending on configuration). VCC allows for automated recording of calls, manual recording of calls, recording of select agents or select skills.

VCC is PCI compliant. VCC provides encryption using an AES-256 compliant encryption to protect calls from unauthorized access and provides the ability to not capture/automatically insert white noise when sensitive data is being captured by the agent.

VCC provides many tools to remove the capture of sensitive data from Audio (and screens, if applicable utilizing optional features) recordings:

- FTP/SFTP Transfer: Call recordings that potentially contain PCI data can be encrypted at rest or clients can request these files be moved off of the VCC platform from SEA (Secure External Access) the client location.
- Secure IVR: The agent would transfer the caller to a secure IVR that would interact with the caller to receive the PCI data. Once the interaction was completed, the caller would be sent back the agent to finish the call.
- Mask / Bleeplog Feature: The Agent Masking feature within the VCC Agent interface is a feature that allows agents to inject “white noise” or “bleep log” into a phone call recording in order to censor any sensitive information that is being communicated and recorded during the phone call.

  For example, Social Security Numbers, Credit Card Numbers, Medical/HIPAA information, personal information, etc. are all information that customers may want to “bleep” or insert "white noise" over the sensitive information with their recorded phone calls.

  This can be initiated automatically, based on field of focus, page or application, or manually by an agent or process as defined by agency.

*4.2.1.1.4.5 The State may utilize an outbound predictive dialing campaign, at an Agency's request. Please describe your solution's capabilities in providing predictive dialing campaigns.*

## Verizon Response

Outbound Dialing Campaigns, if during discovery are determined to be needed, additional charges may apply.

Outbound offers multiple dialing modes which can be defined through skill parameters on a per skill basis. In addition, specific records can be flagged for Preview Dialing even if they are part of a Predictive Campaign.

- Predictive – dials predictively for every available agent to increase agent productivity and the chance of a live connection. The agent is connected to the most progressed call and will hear the first hello from the customer and can immediately respond.

  Other calls that were ringing at an agent’s station will be “hopped” to another available agent, if answered.

  In extreme cases, if no agents are available, the call will be abandoned and the defined abandoned message will be played. Machine detection is employed during the call so the agent doesn’t have to disposition these calls.

- Progressive – Similar to Predictive except that only one call is dialed per available agent to guarantee that no call is abandoned.
- Preview (without timer) – each record is presented to an Agent for review. There is no time limit before the agent has to dial. The Agent then determines whether or not to dial.
- Preview with timeout – Same as Preview with confirmation required except there is a time limit before the system will automatically dial the number. If the time limit is exceeded and no decision is made by the agent, the record is automatically dialed or discarded per skill settings.
- Agentless/Message Lay-Down –With Agentless, calls are made without a connection to an agent for the purpose of leaving a message, playing information or anything that a Studio script can do (IVR/Self Service/Change or check flight status, delays, etc.).
- Manual – users can manually dial numbers and equate the call to a skill for reporting purposes.

It is important to note that Predictive outbound dialing is patented and removes the awkward delay that is inherent in other predictive dialing solutions, creating a better experience for the agents and the patron.

Given the States Response to questions in Addendum 2 & 3 where the response includes that "discovery is a part of the RFP" related to optional hosted Contact Center features, Verizon will undertake discovery upon award and those items not disclosed by the State will be evaluated for effort and potential modifications to pricing may be required to add the services identified.

*4.2.1.2 Security for Vendor's Hosted Solution*

*The State's goal is to ensure the Vendor's solution adheres to industry standard security practices and provides for sensitive data protection (where required) as it relates to cloud-based services. As such, the Vendor should:*

***4.2.1.2.1 Describe how its solution leverages high security standards associated with regulated data and/or high availability requirements, but also offers a cost-effective, standard-security solution option to the state.***

## Verizon Response

### Standard Security Hosted Voice

Verizon's Standard Security Hosted Voice platform uses a multi-customer infrastructure versus a multi-tenant infrastructure.

A multi-tenant infrastructure features a single set of applications in one IP address space on a server (or set of servers) that supports multiple customers.

By contrast, the multi-customer infrastructure used by Verizon provides each customer with a dedicated, virtual instance of each individual application through the use of virtualization technology.

This completely isolates each instance of software from every other instance. Applications run in their own address spaces, with dedicated server processing provided to each customer. The use of virtual routing and forwarding (VRF) technology and individual firewall instances at the edge of the network enables customers to set up their own filter rules.

Data stores in the storage area network (SAN) feature a logical unit number (LUN) dedicated to each customer. This multi-customer environment allows customers to enjoy the benefits of dedicated software while taking advantage of shared hardware, with carrier class security, flexibility, and resiliency.

Verizon uses the industry-proven best practice of a defense-in-depth security model. This model features multiple layers of security and different techniques that provide overlap protection.

Verizon utilizes a variety of techniques and technologies to protect the core network and customer networks. This includes the use of stateful and redundant firewalls, Deep Packet Inspection (DPI), individual server and component hardening and physical security at the data centers.

The Hosted Voice data centers house the infrastructure in a secure, fully redundant architecture. Customer separation within the data center begins at the edge where the Verizon MPLS network ingresses and terminates on fully managed Cisco Nexus 7000 switches.

Customer traffic is then segregated into dedicated virtual LANs (VLANs) within the Nexus and switched into a Cisco ASA firewall where a customer-specific firewall context will permit only traffic destined for the hosted voice platform.

Development of the customer-specific rules begin in the low level design process and is developed in conjunction with the customer and with the customer's feedback

Traffic allowed to pass through the firewall is then switched into new, separate VLANs for voice and data with QoS to prioritize signaling and voice traffic end to end.

Additionally, the session border controllers (SBCs) included as part of the service adds topology hiding and security features to help protect Voice over IP (VoIP) devices that must interconnect with the PSTN.

Finally, the UC applications for a customer are deployed in customer-dedicated instances and provisioned into a customer-owned IP address space. Since the Hosted Voice instances are provisioned only over MPLS, the data centers look and feel like an integral part of the customer's private network.

The deployment model is identical to what customers have historically deployed on their own compute space except the service is delivered out of Verizon's data centers. This deployment model offers customers the best of both worlds; the traditional, robust architecture they are accustomed to having but priced in a consumption model.

The ports and backplane used to communicate between virtual machine (VM) instances and the SAN is segmented like the VLANs that carry voice and data traffic, and distributed switching further isolates customer traffic.

At the compute layer, system resources such as memory and CPU cores are dedicated to a specific customer instead of applications.

A single customer logical cluster of applications is divided in two, and the use of clustering over the WAN distributes the two halves of the cluster between data centers to help prevent a catastrophic event at one location from impacting the entire platform.

In addition, within each data center, the virtual applications are distributed over multiple physical servers to avoid the risk of one device loss bringing down that data center. All customers are provisioned in this geo-redundant mode.

The underlying virtual Linux OS environment has been hardened by the manufacturer to disable all unnecessary services and ports. This appliance model restricts direct access to the OS, instead forcing administration through the management portal.

The entire application environment is also monitored and logged using SNMP and syslogging. In addition, Verizon adheres to industry standard development best practices for the applications and follows all Product Security Incident Response Team (PSIRT) guidelines for known security vulnerabilities and remediation.

The platform is hosted in Tier 4 data centers with multiple layers of physical isolation, requiring a combination of biometric scans, an ID card, and ticket/notification to enable access and work on data center infrastructure.

All servers and network components are protected by a two form factor access method to restrict and actively control access to components.

Furthermore, the Hosted Voice platform is not provisioned to be reached via direct Internet access, requiring the use of dedicated MPLS interconnects to the individual customer's private network.

This provides additional security to the Hosted Voice core by isolating the platform from the Internet. This helps protect the platform and also protects the customer environment by not introducing backdoor access into the customer's MPLS network.

For customers that would like to take advantage of mobility features, Verizon offers the use of Cisco Expressway built into the Hosted Voice environment.

Expressway is a secure firewall transversal solution that allows fully encrypted communications between remote Jabber devices and select Cisco phones and the platform.

Expressway works by leveraging two separate devices Expressway C (Core – inside the network) and Expressway E (Edge – in the DMZ). These devices maintain a secure tunnel between them and force all traffic to pass via this secure, encrypted tunnel.

DNS is used to direct user devices to establish communications with the E server. A secure, encrypted tunnel is set up, and all signaling and RTP traffic is encrypted between both endpoints.

The Internet connectivity at the data centers is used only for Expressway, and we do not allow non-Expressway traffic to use this for any other purpose.

### High Security Hosted Voice

The High Security Hosted Voice solution includes the security described for the Standard Security platform and adds additional security to meet the stringent FedRAMP requirements. FedRAMP provides a standardized, cost-effective, and risk-based approach for the adoption and use of cloud services by US government agencies.

FedRAMP processes are designed to assist federal government agencies in meeting Federal Information Security Management Act (FISMA) requirements for cloud systems.

By standardizing security assessment, authorization, and continuous monitoring for cloud products and services, this program delivers cost savings, accelerated adoption, and increased confidence in security to US government agencies that are adopting cloud technologies.

This platform is FedRAMP Authorized at the Moderate Impact Level. State and local governments can also take advantage of this secure platform to meet their high security needs.

The data centers providing this service are physically separate from the data centers used to provide the standard security Hosted Voice solution.

All support mechanisms and personnel are dedicated to this solution and are also separate from the standard security solution. Inside the data centers, the applications are logically separated from other customers in a similar manner to the standard security platform.

All endpoints must support FIPS 140-2 encryption. FIPS 140-2 compliant, end-to-end encryption is utilized for sensitive data transmitted outside of the data center boundary to the end user and for application and tools traffic inside the data center.

All data at rest inside the data center is encrypted to this same standard. Calls bound for the PSTN are unencrypted since the PSTN does not support encryption.

This platform is subject to audits by an independent FedRAMP third party assessment organization.

### Private IP Security

Commercially available as a service option since 2000, Private IP is Verizon's Multiprotocol Label Switching (MPLS)–based, Layer 3 VPN service. The solution connects customers to their disparate locations around the globe, providing flexible and robust design options while also offering the ability to interconnect with complementary Verizon services.

Private IP service is based upon RFC 4364 and provides Layer 3 VPN services over a MPLS architecture. MPLS can be a powerful tool and is used for three main reasons:

- Engineering the network core more efficiently (manages capacity and congestion, provides traffic routing control and prioritization)
- Providing VPN services (e.g., MPLS VPNs)
- Enhancing network resiliency through the use of MPLS Fast Reroute

While Private IP (and MPLS itself) is widely accepted within the industry, many businesses are still unfamiliar with the protocol, specifically when it comes to security. Because of this, questions concerning Private IP's security regularly arise in our everyday discussions with clients.

This explanation aims to provide an overview of Private IP security by looking at general MPLS security components, as well as the Verizon Private IP service architecture itself.

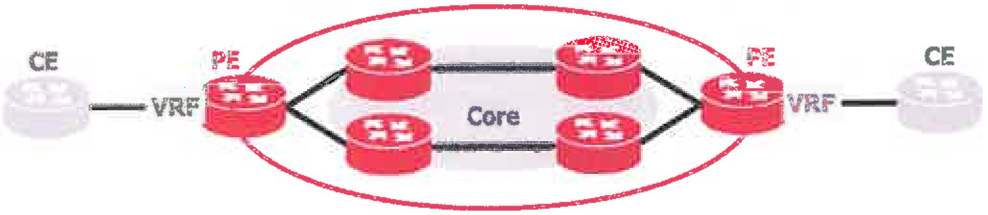
This document provides a high-level definition of MPLS and the basic security components built into its framework—as well as the Verizon Private IP architecture and additional measures related to it.

However, this document does not address security related to the various access methods and network interconnects that are available with Private IP. These components will be addressed separately in another document.

### High-Level Verizon Private IP Architecture

The Verizon Private IP service is based on RFC 4364, which describes a method for providing VPN services over an MPLS and IP backbone. The key physical and logical components are described below.

P-Core



*High-level Private IP architecture*

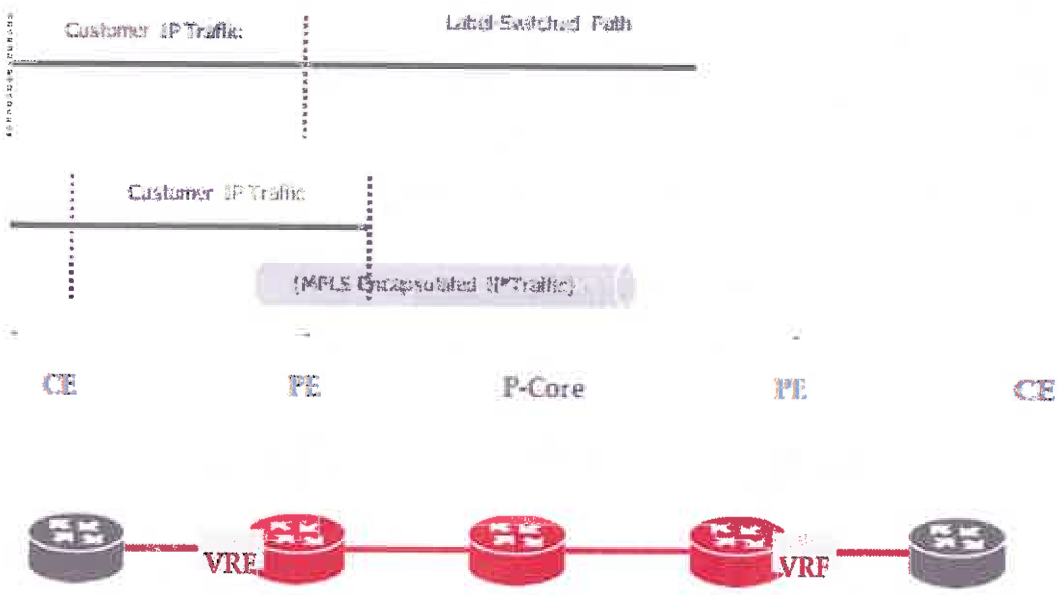
- **Customer edge (CE) router.** The customer edge router is the IP router at the customer premises. This is the device that connects to and peers with the provider edge (PE) router. CEs do not peer with each other. CEs are considered part of the customer's VPN and do not participate in any core routing. The CE is not MPLS-aware and is only configured for standard IP routing.
- **Provider edge (PE) router.** The PE router resides in the service provider's (Verizon's) core. The PE learns IP routes from the CE, usually via a dynamic routing protocol, and stores them in a separate Virtual Routing and Forwarding (VRF) instance for each connected CE interface.

  An 8-byte route distinguisher (RD) is prepended to every IP address to create globally unique VPN-IPv4/v6 addresses. The PE uses Multiprotocol BGP (MP-BGP) to distribute VPN-IPv4/v6 routes to other PEs in the customer's VPN.
- **Virtual Routing and Forwarding (VRF) instance.** The VRF is effectively a separate routing table per customer VPN—many VRFs exist in every PE. VRF membership is determined based upon the ingress interface on the PE. A customer's VPN is then the collection of the participating VRFs.
- **Provider (P-core) router.** P-core routers are those routers in Verizon's backbone that do not connect to CE routers and, in most cases, form the core of the network. P-core routers are not VPN-aware (do not contain any customer routes) and only forward MPLS-labeled packets between PEs.

A high-level, simplified description of customer data flow is described below. Customer traffic enters the network at the CE and flows toward the PE, with which it peers across an access network. The PE router maintains a VRF, which is associated with the ingress interface and will contain advertised customer networks.

MP-BGP is used to distribute routing information between PEs. The MPLS protocol then encapsulates the IP data, adding labels, and switching traffic along pre-signaled label switched paths.

The MPLS encapsulated traffic arrives at the far-end PE, where the labels are removed and the customer's IP traffic is sent across the access network to the destination CE.



*High-level Private IP data flow*

### Security Requirements of MPLS Networks

The following sections will describe the inherent security mechanisms built into the VPN service provided by Private IP—characteristics that are traditionally associated with Layer 2 VPNs. MPLS security is based upon three basic principles:

- Necessity for address and routing separation
- Keeping the internal structure of the core network hidden from the outside
- Providing resistance to attacks

### Address Space and Routing Separation

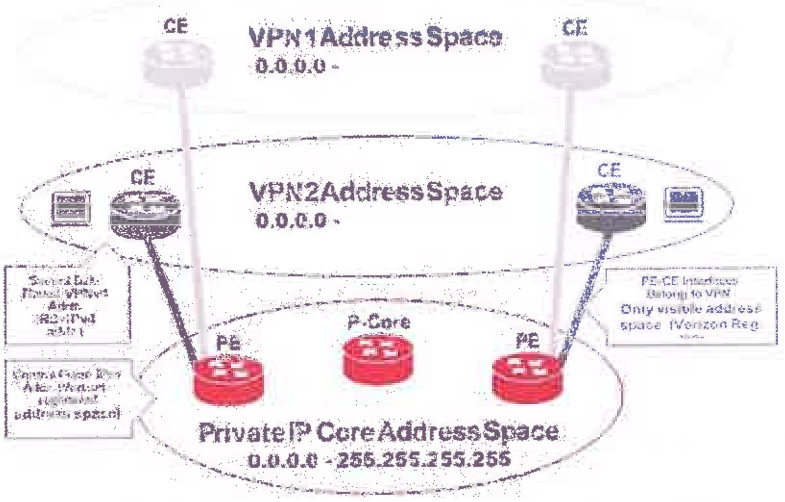
MPLS-based VPN services must provide customers the flexibility of maintaining their own unique addressing plans and freedom to use either public or private address space.

This means that between any two non-intersecting VPNs, the address space between these different VPNs is independent.

For example, two separate, non-intersecting customer VPNs would be able to use the same 10.0.0.0/16 network without fear of conflict. From a routing perspective, this means that each end system in a VPN has a unique address and all routes to this address point to the same end system.

Specifically,

- A VPN must be able to use the same address space as any other VPN or the MPLS core.
- Routing between any two VPNs must be independent.
- Routing between any VPN and the core must be independent.



*Address and routing separation*

- **Address space**. Private IP service allows distinct VPNs to use the same address space, which can be publicly registered or private IPv4 address spaces (RFC 1918). Customers also have the option of using IPv6 addressing obtained either directly from ARIN or their ISP with the Private IP service.

  This address uniqueness is made possible by adding a 64-bit RD to each IPv4 or IPv6 route, making these addresses not only VPN unique but also unique across the MPLS core. This address is also sometimes called a "VPN-IPv4 address" or "VPN-IPv6" when IPv6 addressing is present.

- **Routing separation**. Routing separation between Private IP customers is provided by each PE router maintaining a separate routing table for each connected VPN—or a VRF instance. The VRF contains only the routes for the VPN that it is associated with and that were learned either statically or through a dynamic routing protocol (e.g., BGP, RIP).

  These VRFs are also separate from the global routing table. The Private IP core does not contain customer routes, but only those routes required for providing core reachability. These individual VRFs are further secured through the use of import and export targets with MP-BGP.

  A customer VPN is configured with a specific set of route targets and the associated VRFs only import/export routes for the specified VPN, helping protect them from non-customer route injections.

VPNs only contain routes associated with their corporate VPN. If identified during discovery that routing separation is required, additional costs may apply.

### Hiding the MPLS Code Structure

The second security principle of MPLS-based VPN design requires that knowledge of the core of the network is limited or completely hidden from the outside.

In general terms, if a potential attacker does not know the detail (e.g., IP addressing) of their potential target, it makes that target difficult, if not impossible, to attack. So, Private IP does not unnecessarily reveal this and other information, even to customer VPNs.

When a dynamic routing protocol is run between the PE and CE (e.g., external BGP [eBGP]), the only information that is required is the address of the PE router. When security requirements dictate even stricter measures, static routing can be configured between the PE and CE, which would allow the Private IP MPLS core to be kept completely hidden.

### Resistance to Attacks

Because of the routing separation provided to Private IP customers, it is impossible to gain access to other VPNs unless it has been explicitly configured (e.g., via an extranet configuration).

The use of MP-BGP and route targets constrain the routing within the VPN only to those routes learned through the customer's CE-to-PE connection (static or dynamic). By design, there is no direct connectivity between the Private IP network and the public Internet.

Private IP PEs are dedicated to providing the private Level 3 VPN service. Furthermore, the Verizon core is dedicated to MPLS switching and does not contain any Internet or customer routes. This architecture design limits the potential for unauthorized users and for external attacks.

Even though the potential for attack may be low and unlikely, the Verizon Private IP MPLS architecture does provide protection mechanisms against the following basic types of attacks:

- Intrusions—Where the underlying goal is to gain unauthorized access to resources
- Denial of service (DoS) attacks—Where resources become unavailable to authorized users

We have already discussed the inherent security provided by limiting customer VPN access to only those sites and interfaces explicitly configured. Through this mode of configuration, it is not possible to directly intrude into other VPNs.

Fully covered in a later section, there are also numerous device-level controls in place that restrict access to and protect the Verizon Private IP service nodes and core from unauthorized use.

These safeguards already provide a great deal of protection from intrusion at both the device and VPN levels. Discussed in the previous section, the Private IP core does not reveal unnecessary information about itself (e.g., addressing), which helps further protect against unwanted attention and access.

The option of configuring static routing also exists, whereby the PE routers are manually configured with only those routes to specific customer networks listed behind each CE. The CEs themselves are then configured to statically point to the PE router for any network in other parts of the VPN (mostly a default route).

If the CE-configured route to the PE points to the local interface, the CE router doesn't need to know any IP address of the core network, not even of the PE router. Taking these optional steps provides additional levels of network security, as it is only visible and accessible to those resources and individuals who need it.

To help reduce the risks of DoS and unauthorized intrusion, the PE's routing processes are securely configured. This is done in various ways:

- Access control lists (ACLs). ACLs are used on Private IP interfaces to restrict the routing protocol to only the CE router and nowhere else. Furthermore, ACLs are used to limit access to the PE from only known entities.
- Parameter configuration. Where practical, PE configurations are given parameters that are tuned to further secure communication. For example, Private IP VRFs are configured with a maximum number of routes, which helps to protect the router from receiving an abnormally large number of routes in a DoS attempt.
- MD-5. This is an optional configuration for authentication for routing protocols. This is available for BGP (RFC 2385) Private IP customers. It avoids the packets that could be spoofed from other parts of the customer network than the CE router.

This requires Verizon and the customer to agree on a shared secret between all CE and PE routers.

In summary, Verizon's PE routers offer multiple levels of security, especially on their interfaces to the CE routers. ACLs are configured to limit access only to the port(s) of the routing protocol and only from the CE router. MD-5 authentication is an optional customer configuration item and can be used on CE-PE peering.

### Label Spoofing

Within the Private IP service core, network packets are forwarded based on labels that are prepended by the PE routers. The interface between any CE router and its PE router is an IP interface.

The CE router is unaware of the MPLS. The "intelligence" or MPLS switching is all done within the PE device and the Private IP core. Because of this, a PE router will not accept a packet with a label from a CE router. Labeled packets arriving from a CE will be dropped by the receiving PE. As such, it is extremely difficult to insert or spoof "fake" labels.

### Additional Security Controls

While the inherent security mechanisms built into the Private IP MPLS architecture discussed in this document are typically sufficient for most customers and their security environments, there are always cases where additional security measures are warranted.

This may be driven by simple perception or additional industry security requirements within HIPAA or PCI DSS. If further security safeguards are necessary, several customer-configurable options exist for use.

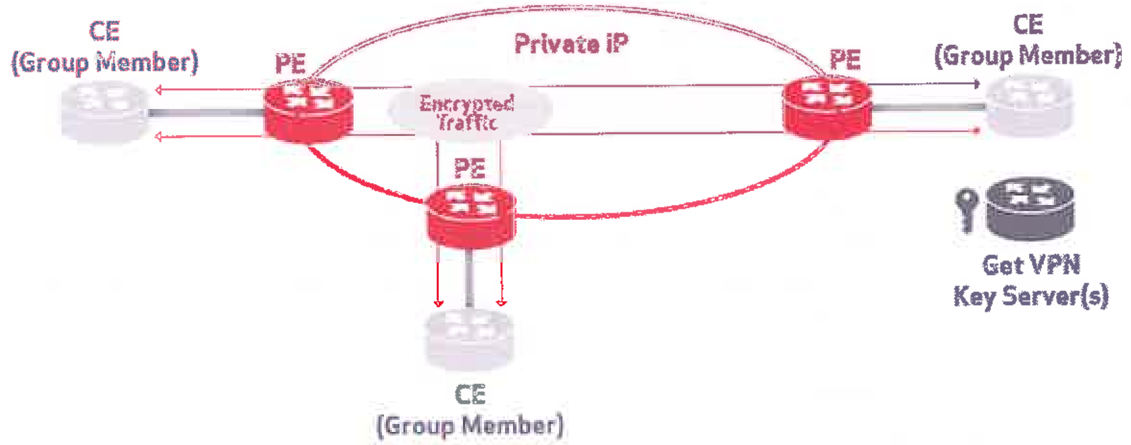
While it is not within the scope of this response to discuss these additional customer network–level security designs in detail, it is worth noting common options which may be employed.

- MD-5 authentication – An optional configurable parameter, MD-5 authentication is available for Private IP customers using eBGP as the CE-PE routing protocol.
- Configuration of static routing on CE-PE connection – When hiding the Private IP core becomes paramount to protection, static routing may be configured on the CE-PE link. When done, no Private IP information (PE addressing) is revealed to external devices.
- Customer-managed encryption – The Private IP network does not provide encryption services itself; however, customers have the option to configure encrypted CE-CE tunnels when their internal security requirements require this.

  Options include point-to-point GRE + IPsec, Dynamic Multipoint VPN (DMVPN), and GetVPN.

  GetVPN is particularly well suited to private WAN environments like Private IP because the technology is "tunnel-less" and uses the original IP header to take advantage of existing core routing and quality of service (QoS) support.

  Direct IPsec encryption and DMVM tunneled designs that hide the original IP header and addressing are also supported when situations warrant.



*GetVPN "tunnel-less" encryption option*

- Verizon security standards. Verizon has several internal organizations that provide support functions for the Private IP network.

  All of these internal groups and their personnel have strict policies and controls in place to allow secure communication with and support of the Private IP architecture. These groups range from ordering and provisioning to monitoring, reporting, and service on the network once in place.

  Over all of these groups and components, Verizon's internal security organization and the Verizon Network Security Operations Center (NSOC) has primary responsibility for internal security policies and their enforcement.

- Verizon security organization. Verizon's security organization has developed a consolidated approach and set of controls so that the Private IP service operates within designed levels of confidentiality, security, and availability.

  The security organization is responsible for the protection of all company assets, facilities, and information, as well as providing for those policies governing employee access for support of the Verizon service network.

  Preventing incidents before they occur may be the most important aspect of Verizon's security plan. To this end, Verizon has in place a continual process of identifying, measuring, and implementing safeguards to reduce risk of an event impacting the integrity or availability of the Private IP service.

  This process involves the regular scanning of internal systems and networks for vulnerabilities and remediation of any gaps found within.

  This is based on current understanding of existing and upcoming threats and risks within the industry and through direct participation in several security associations and continual research.

### Personnel Safeguards

Verizon bases its own internal personnel security mechanisms upon widely accepted best practices.

Verizon policies provide for the following:

- Verizon pre-employment screening and mandatory drug screening
- National Industrial Security Program requirements for U.S. government employees
- Ongoing security training and awareness covering a range of topics

The personnel security program provides clear roles and responsibilities for employees based upon the definition of their job function. Employees are only provided access to internal network and devices based on need as defined by their function.

Whether due to normal termination of a job function (e.g., short-term, contractor) or other reasons, network access is swiftly removed per company policies so that access is available only when specifically required.

### Verizon Physical and Environmental Protection

The physical protection of the actual facilities that house Verizon network equipment and systems is just as important to the overall security architecture as protection from network-level threats.

Verizon categorizes physical security at several levels. The first two levels address those areas of a facility where the public may have access. This is the building perimeter and internal public space.

These areas use appropriate signage, barriers (locked doors, manned desks, and turnstiles), and badge readers among other mechanisms—so that individuals are made aware they are entering a secured area.

The third security level is defined as the employee space and is accessible only by workers and contractors as needed to conduct their work.

The fourth level is the highest security level assigned to facility access and is reserved for those locations and areas that house Verizon assets and information that may be accessed only by select employees.

The Private IP network nodes are provided this level-4 protection, which includes these additional components:

- Personnel access controls, including access lists and badging—as well as the ability to authenticate active employees against HR records
- Physical protection using guard services, electronic card readers, and surveillance cameras

- Protection through physically limiting access to network terminals and resources, as well as sensitive software and documentation
- Physical controls during software development and related activities to help protect the software that is used for handling customer-sensitive information and data

### Private IP Device–Level Safeguards

Numerous controls have been put in place to help protect Verizon network devices from unauthorized access and the inadvertent or malicious modification and destruction of data.

At a high level, direct access to the Private IP PE routers is not permitted, and access is allowed only across the Verizon internal data network. Mechanisms include, but are not limited to:

- ACLs restricting access to required external devices and services only
- Turning off all unnecessary interfaces and services
- Internal Verizon user access limited to required personnel only, which is constantly monitored using two-factor authentication
- Logging of user actions on Verizon equipment with further controls allowing for administration and restriction of privilege levels, recording, and review of actions
- Performing configuration changes associated with provisioning or customer service via automation or application access whenever possible to help reduce the chance of manual error
- Backups of device-level configurations and other critical files, as well as regular testing of disaster recovery and restoration processes conducted on a regular basis

### Private IP Network Architecture Assessment

Verizon underwent an in-depth network assessment with Trustwave in 2013, aiming to review documentation and physical security relative to those best practices and safeguards specified under

National Institute of Standards and Technology Special Publication 800-53 Rev. 3. While not an accreditation, the Trustwave assessment did report that the Verizon Private IP architecture was in compliance with all security control families that were applicable.

### Summary and Conclusions

The Private IP service provides full address and routing separation that meets that which traditional Layer 2 VPN services have achieved. By design, Private IP does not reveal the addressing structures of the core or other VPNs, and its security controls help prevent intrusions into the core or other VPNs by abuse of MPLS mechanisms.

Verizon has put in place an internal security organization to help implement the proper controls, so that the Private IP service operates within designed levels of confidentiality, security, and availability.

For environments that require stricter control measures, additional optional security mechanisms may be put in place to meet customers' unique internal needs. Customer-managed CE-CE encrypted tunnels, such as GetVPN or point-to-point or multipoint GRE + IPsec, are one such option and are supported across Private IP.

It should be noted that the overall security of any architecture depends on all solution components. While the Private IP service includes many security controls and features, public Internet access, remote access solutions, and traditional internal network access must also be secured to help prevent compromise to your network design.

*4.2.1.2.2 Describe its policies and procedures for conducting sub-contractor assurance, validating both the capability of the vendor to fulfill contracted responsibilities and adhere to all applicable to security & privacy policies and controls of all parties.*

## Verizon Response

Verizon's National presence and footprint along with our strategic Partnerships allows Verizon to provide the desired coverage in a multitude of facets.

Verizon's goal to the State of West Virginia is to provide the highest level of service and satisfaction, so Verizon will engage all resources needed to meet the demands and desires of the State.

In areas where we don't have direct support, Verizon has solid relationships with the largest, strongest sub-contractors on a national basis. All Verizon sub-contractors provide services on behalf of Verizon and under strict supervision of Verizon.

Verizon's rigid guidelines ensure only quality vendors that are stable in size, that provide quality service. Verizon's Legal team reviews and approves all Subcontractors applicants to ensure compliance. All sub-contractors will have the appropriate level background checks.

For up to date information on third parties, Verizon maintains a database that contains Carrier and Supplier Contracts, Products and Provisioning and Repair information.

Verizon also maintains a Carrier Scorecard in which several metrics are used to evaluate third party carrier performance.

*4.2.1.2.3 Describe its company's cyber security and privacy management program including an overview of the governance structure, cyber security strategy, and the experience of personnel in key security and privacy roles.*

## Verizon Response

Please reference the Cyber Security Program documentation provided in Appendix E of this proposal.

*4.2.1.3 Service and Support for Vendor's Hosted Solution*

*The State's goal is to partner with a Vendor whose service and support structures allow the State to focus on its core services, while ensuring telephony and contact center systems are available to State Agencies, with certain Agency sites (hospitals, jails, etc.) operating critical services 24x7x365.*

*The State desires a Vendor to provide all levels of tiered support, including Tier 1 support for end-users. To this end, the Vendor's service and support structure for the Vendor's hosted solution should provide for the following:*

*4.2.1.3.1 Performance monitoring, capacity planning, and real-time surveillance of the Vendor's network to ensure 99.9% availability of services and provide network utilization reports upon request.*

*Please describe your company's process and ability for providing this information upon request, including any lead times needed and how the State submits these requests.*

## Verizon Response

Verizon is proposing a comprehensive solution to the State of West Virginia, with 24 hour coverage and support to the end user.

Verizon will provide network monitoring to include capacity planning and management, and utilization reporting. Additionally, the State of West Virginia will have access to data and information via the VEC.

The Program Management Office (PMO) will be the single point of contact for Service, reporting and billing administration.

The State of West Virginia will have the ability to request service support directly through the VEC, and in partnership with the PMO. During transition phase, clear roles and responsibilities and process details will be defined and mutually agreed upon.

Please reference the Account Service Plan provided in Appendix I for roles and responsibilities. This response includes Monitor & Notify with the Ethernet Access to Private IP.

*4.2.1.3.2 The State desires regularly scheduled meetings and/or calls to discuss the following areas:*

- *Architecture and Design*
- *Implementation*
- *Ordering and Billing*
- *Service and Support*
- *Project Management*

*Please describe your company's ability to hold regular meetings on each of these topics, as well as your company's implementation plans for starting these discussions.*

## Verizon Response

Verizon Program Management Office will organize and facilitate status and performance meetings. Through the Verizon governance model, committees will be formed and designed according to the final solution and contractual commitments.

The committees will include members of key Verizon and State of West Virginia team members. Verizon team members will lead and organize the meeting schedule and agenda, and facilitate to resolution, release meeting minutes, and next steps accordingly.

*4.2.1.3.3 Vendor should contact the State's engineering points of contact by phone within 30 minutes of a Vendor network outage that affects multiple sites on the State's network.*

*This verbal notification should be followed with a written report that provides an explanation of the problem, the cause of the problem, the solution to the problem, the estimated time for recovery, and the steps taken or to be taken to prevent a reoccurrence.*

*To that end, please describe your company's notification procedures in the case of an outage.*

## Verizon Response

Verizon will provide the Monitor Notification services that are in place today.

Verizon Monitor and Notify Service manages:

- Monitoring if the PIP network access circuits
- Fault Notification:
  - Sends an email to the customer and Verizon account team of any access circuit faults
  - Automatically opens a trouble ticket with the Verizon NOC
  - Verizon Service Manager follows the fault event providing the customer with status reports though fault resolution
- Asset Reporting
- Performance Reporting

*4.2.1.3.4 Vendor should provide written notification of ten (10) business days or more in advance of any planned upgrades, modifications, etc. that may affect the State's customers to the State's engineering points of contact. Please describe your company's notification process for planned maintenance.*

## Verizon Response

Verizon Scheduled Maintenance has three types of customer impacts. High risk maintenance activities that will result in a service disruption of greater than 50 milliseconds require 10 business days advance notice.

There are two lower risk activities that result in a service disruption of less than 50 milliseconds or no disruptions requiring 48 hours advance notice.

*4.2.1.3.5 Vendor should provide notification of three (3) business days or more in advance of emergency maintenance. While the State understands emergency outages and/or unplanned maintenance windows occur, it is expected that these situations are kept to a minimum.*

*Please describe your compan y's notification process for emergency maintenance and outages.*

## Verizon Response

The Service Manager will communicate impacts as a result of emergency maintenance change activity. The process will be designed through the governance model, identifying key members, steps and time frames.

*4.2.1.3.6 If the Vendor's work requires them to be at a State site, the Vendor should provide Agency at least 72 hours' notice before arriving at the site and comply with State law and all Agency policies, including but not limited to background checks for contractors, vendors, and visitors.*

*Please describe your approach and methodology in your solution/response.*

## Verizon Response

The PMO will provide oversight to any Verizon contractors and will coordinate scheduling on-site work with the State of West Virginia. The Verizon PMO will work with the contractors to ensure their personnel have completed appropriate background checks.

*4.2.1.3.7 The Vendor's network operation support center should provide: all tiers of support, including end-user support, advanced technical expertise, be staffed with resources that are proficient in spoken and written English, maintain and take responsibility for trouble tickets reported by the State until resolved, and provide a tiered support escalation process.*

*Please describe your network operation support center's structure, processes, and procedures for handling trouble tickets, resolving those tickets, and reporting back to the State's point of contacts.*

## Verizon Response

### Trouble Tickets & Repairs: Contacting Customer Service & the Service Desk

Once UCCaaS implementation is complete, your service is supported by customer service, the UCCaaS Service Desk and Tier 2 NOC personnel.

**Reactive Incident Management**

The assigned contact number serves as the entry point for customers to report problems or troubles. This group will evaluate the service report and engage the UCCaaS Service Desk for UCCaaS specific troubles. The **UCCaaS Service Desk** owns the trouble report from there and provides hourly updates on outage tickets. The Assigned Customer Service Desk will also be the point of contact for updates on trouble tickets or to request escalations.

**Proactive Monitoring & Trouble Ticketing**

Most incidents are proactively detected and ticketed by the Verizon management systems. You may occasionally encounter issues that aren't detected by Verizon systems. In those situations, please report the problem using one of the methods listed below. A Customer Service representative will refer customer-initiated tickets to the appropriate NOC.

**When there is a functional problem, such as an outage**, please contact us per below. The best way to open a trouble ticket is online at the VEC (Verizon Enterprise Service Center) using your UCCaaS SIID.

| | |
|---|---|
| **VEC (Verizon Enterprise Service Center)** | **https://enterprisecenter.verizon.com**<br>**Customers can open tickets, check status, view service agreement status and more.**<br>**Please see: Appendix B: Instructions for Opening Trouble Tickets for Non-Verizon TNs/Local Gateways if your TN is not provided from Verizon.** |

| | |
|---|---|
| **United States** | US customers dial see below. This is a fast, efficient way to get your issue ticketed. This is the same number dialed for the Customer's existing services.<br>Note to be deleted prior to giving to customer:<br>The number provided to customer may vary based on their managed network services status:<br>· For existing managed services customer, use the incoming call group to determine the correct phone number.<br>· New managed services customer see the MNS Fulfillment Letter (if not yet in ESP) to determine the incoming call group. |

***WHAT VERIZON NEEDS WHEN ISSUES ARE REPORTED***

Please have the following information available before placing a call or opening an electronic ticket. <u>Emphasize that you are calling about UCCaaS service.</u>

For Service or Repair:

- Customer Contact Name
- Customer Contact Telephone Number
- Customer Contact E-mail Address
- Directory Number/Telephone Number (DN/TN) of user(s) impacted (When entering online into the Verizon Enterprise Center, this may require entry of country code or a leading, such as 1NPANXXXXXX)
- User(s) Location/Site information
- Calling and Called party numbers, Time of day, Number of failed call attempts
- IP Address (source and destination if available), MAC Address (if available)
- Brief description of the problem/symptoms (failed registration/no dial tone etc.) including any steps taken to identify the problem or resolve the issue

### Customer Responsibilities

Verizon's Service Desk and Network Operations Center (NOC) provide Level 2/3 support for customer administrators. As such the customer has the following support responsibilities:

- The customer must designate an administrator or administrators responsible for reporting trouble incidents as well as submitting authorized change management requests. The customer shall have sufficiently trained personnel on the use and application of the product who can perform this function
- Before requesting support, the customer must verify that the problem is not being triggered by items not covered within the Support Contract

### Customer Expectations – Trouble Ticket Severity

When an issue is initially reported, a trouble ticket will be opened. Once the initial ticket information is gathered and support coverage is verified, a ticket number will be generated. This ticket number will be provided to the caller or sent via email.

Customers should refer to the ticket number when referencing an issue in all future communications. We also recommend that the ticket number be included in the subject line of any email correspondence.

Service/Outage Definitions:

| | |
|---|---|
| Critical Problem | Application(s) down, access to application(s) down or intermittent issues affecting all users. (All users would be all locations) |
| Incident | Intermittent trouble or trouble affecting single user reported, single location issues or single location down |
| Inquiries | Request for information regarding the UCCaaS service (i.e.: feature configuration) |
| Resolution | Remediation of a problem to a customer's satisfactory conclusion |
| Response Time | Time required to react and resolve to reported problem, incident or inquiry |
| Work Around | Reported problem or incident has not been resolved but configuration or feature changes provide an alternate solution to support service until the problem is fully resolved. |

Tickets are assigned the following priority levels, with the associated response times.

| Priority level | Response time | Definition |
|---|---|---|
| P1 | 4 hrs | 50% or more of total applications out of service<br>All international outages<br>Inability to complete to a single or multiple users<br>50% or more of the location is out-of-service.<br>50% or more of the ports/channels are out-of-service.<br>Network outage with multiple customers affected.<br>Critical system failure with multiple customers down.<br>Equipment inoperable with no workaround capability with multiple customers affected. |
| P2 | 8 Hours | Less than 50% of total applications out of Service<br>Any completion problems<br>Less than 50% of the location is out-of-service.<br>Less than 50% of the ports/channels are out-of-service.<br>Major/Slow performance issues.<br>Single critical customer (1 user) is down with no Restoral.<br>Major/Slow network performance issues. |
| P3 | 24 Hours | Single incident service inquiries<br>Single or multiple customers affected, but there is a clear workaround capability.<br>There are intermittent problems.<br>The impairment allows the customer to continue to function.<br>Slow performance issues that are not a major issue with the customer. |
| P4 | 72 Hours | Preventative maintenance service inquiries and MACD requests<br>Non-intrusive reason for outage<br>Not service affecting.<br>Scheduled maintenance and repair.<br>Scheduled upgrade.<br>Single User Change Management Requests |

### Ticket updates

Customers are encouraged to check the Verizon Enterprise Center for ticket status and updates BEFORE requesting an update from a Service Desk engineer. If there are additional questions about the status, then an update request should be made to a Service Desk. Always refer to a specific ticket number when requesting updates.

## 24 X 7 Escalations

Verizon's objective is to restore services to their normal operating conditions as quickly as possible. To accomplish this goal, the Service Desk uses escalation guidelines. If at any time an issue is not progressing to a customer's satisfaction, customers can call into the Service Desk to request an escalation. The appropriate Shift Lead or Supervisor will be notified.

*4.2.1.3.8 The Vendor's solution should include a documented support and escalation structure to address outages. The State prefers the severity of the issue/support problem to determine the average problem resolution response time, as outlined below:*

- *Severity Level 1 is defined as an urgent situation, where the customer's services are unavailable and the customer is unable to use/access the network. The Vendor should resolve Severity Level 1 problems as quickly as possible, which on average should not exceed two (2) business hours.*

  *If repair inside the 2-hour window is not feasible, then regular 1-hour updates are desired.*

- *Severity Level 2 is defined as significant outages and/or repeated failures resulting in limited effective use by the customer. The service may operate but is severely restricted (i.e. slow response, intermittent but repeated inaccessibility, etc.).*

  *The Vendor should resolve Severity Level 2 problems as quickly as possible, which on average should not exceed four (4) business hours. If repair inside the 4-hour window is not feasible, then regular 2-hour updates are desired.*

- *Severity Level 3 is defined as a minor problem that exists with the service, but most of the functions are still usable, and some circumvention may be required to provide service.*

  *The Vendor should resolve Severity Level 3 problems as quickly as possible, which on average should not exceed ten (10) business hours. If repair inside the 10-hour window is not feasible, then updates are desired at the start of the next business day and every day thereafter until repairs are complete.*

*Please describe your company's severity level structure, as well as your documented procedures for handling outages, including escalation processes, notification methods, and resolution times.*

### Verizon Response

The Service Manager will be engaged on any service support issues and participate as a team member in issue and escalation resolutions. The Service Manager will assist in engaging key resources needed for issue and escalation resolutions. See Response Above, 4.2.1.3.8.

*4.2.1.3.9 The State desires the ability to place initial service orders, any changes with an associated charge, or to disconnect services, electronically and receive confirmation of receipt and subsequent order detail. The State desires details including the following data elements:*

- *Telecommunications Change Request (TCR) Form Number*
- *Date order was received*
- *Customer Name*
- *Customer on-site address*

- *Projected due date*
- *Rate element identifier (circuit ID or other)*
- *Additional order details*

*Additionally, the State prefers the Vendor's solution has a web portal for Agencies to enter moves, add, and changes that do not contain billing elements. MACD changes should be resolved by the same or next business day.*

*Please describe your company's ability to accept, process, and report on electronic order submissions, as well as any requirements from the State needed to implement such a program.*

## Verizon Response

Initial Service orders will be handled by the Account Team via the TCR process. Depending on the specific service, a toll free number and/or an online portal will be provided for disconnects, moves, adds, or changes (MACDs).

*4.2.1.3.10 The State maintains a Learning Management System (LMS) for training purposes. The State desires web-based training and training materials for all services offered under this contract.*

*The State desires the Vendor to provide materials that can be uploaded into its LMS, initial Train the Trainer session(s), and documentation/reference materials that can be distributed to and used by end-users. The State intends to incorporate these materials into its LMS, as well.*

*Additionally, the State desires training sessions, if requested by the Agency, and the Vendor should include a professional services rate for training that would be above and beyond the initial training included in the site deployment.*

*The expects the Vendor's training materials to be updated as necessary . The training services for the hosted voice services should be included in the monthly per package cost. Please provide information regarding your training program.*

## Verizon Response

**Standard/High Security Hosted Voice and Virtual Communications Express Training:**

There are three options for Hosted Voice services training. One is that OT can provide end user phone training and any additional Administrative portal training the State may require if opting not to use the online instructor led Administrative scheduled classes. Second option is that

Verizon can provide "Train the Trainer" training, and those trainers will train the end users. Third, Verizon will provide end user phone training. Verizon's training would be web based or custom on site requested training via Professional service rates is available and can be referenced on the cost sheet.

Verizon CTD houses up-to-date user guides in the library section, to include how to use the phones selected by the State. The Customer Training and Development (CTD) web site is https://customertraining.verizon.com/ ).

CTD utilizes Instructor Led Training via Live Meeting and Audio Bridge Registration is required, but there is no charge to access the web site once registered. The VEC/CTD portal provides solution specific documentation that can be utilized for ongoing training and supplement the State's LMS.

### Verizon Enterprise Center

The Verizon Enterprise Center (https://enterprisecenter.verizon.com/ ) offers a suite of web-based applications that allows you to streamline business processes and control critical business functions, while having 24x7x365 access to a virtual communications center.

Through applications on the Verizon Enterprise Center, you are empowered with the ability to view, track, and customize the products that help you to run your business.

The Verizon Enterprise Center Portal also contains a comprehensive list of services and products and telephone numbers for all key Verizon points of contact.

The Hosted Voice administrative users guide for the administrative portal is available here: https://customertraining.verizon.com/commercial/ug_uccaas_index.htm .

### Verizon Enterprise Center Registration

It is important to register for your Verizon Enterprise Center access promptly so it is available when needed. Please remember to keep your log in information accessible and secure.

Your Account Team can guide you through the following enrollment process:

Step 1. Your Account Team will verify your contract details. They may need to submit an entitlement request for you, since the Managed Services Portal—ESP entitlement will be required for access to Performance Management Reports when available, as well as ESP short codes.

Step 2. You will then self-register on the Verizon Enterprise Center by following the prompts.

Step 3. The Verizon Enterprise Center will email you a verification code, confirming registration.

Step 4. You will use that verification code to complete the self-registration.

Step 5. Inform your Verizon Account Team you've successfully registered and that your Portal access should be enabled.

Step 6. Your Account Team will notify the Service Management team to enable your Portal access.

To register a user account on the CTD website:

Step 1. Go to https://customertraining.verizon.com/

Step 2. Select the appropriate category: Commercial.

Step 3. Click on HOW TO REGISTER and follow the prompts.

Step 4. Follow the prompts to watch the six-minute automated TRAINING ORIENTATION.

To enroll in a class:

Step 1. Login at https://customertraining.verizon.com/

Step 2. Enter the login name and password you created.

Step 3. Click the EVENT LIST link on the left side of the screen.

Step 4. Select the appropriate category.

Step 5. Find the class name and click the ENROLL link.

Click the USER GUIDES/DOWNLOADS link on the left side of the screen to print user guides or reference material.

On the day of the class:

Step 1. Login at https://customertraining.verizon.com/

Step 2. Click on MY SCHEDULE to see your list of enrolled courses.

Step 3. Click the ATTEND link next to the class in which you enrolled.

Step 4: Call the audio bridge that pops up on your screen.

If you have questions or problems, please contact the CTD team:

- CTD telephone: +1 800 662 1049
- CTD website: Step 1. Login at https://customertraining.verizon.com/
- CTD e-mail: ctd-cos@one.verizon.com

*4.2.1.3.11 The State desires an hourly rate for Hosted Contact Center Training Services in the instance the State desires training sessions beyond the training provided at initial implementation. The training at initial implementation should be built into the one-time costs for the Contact Center.*

*These training services should include training for all contact center roles and should be provided at the State's request. Please describe your Contact Center training offerings and your solution's ability to meet this goal.*

## Verizon Response

Training for the Verizon Hosted Contact Center offering powered by NICE inContact, beyond the training provided at the initial implementation, utilizes the Verizon Customer Training and Documentation (CTD) for Instructor Led Training via Live Meeting and Audio Bridge, Context Sensitive Help within the solution, Online Help, and NICE inContact University at no additional cost.

The Verizon CTD provides training resources for instructor-led training for Virtual Contact Center Administrators, Call Center Managers, and Supervisors. These trainees can attend a two-hour instructor-led class attended via Live Meeting.

The Virtual Contact Center Overview training is provided by CTD and offered at least once a month. In addition to the instructor-led class, CTD has also created a couple of short tutorials on VCC Reporting.

### Documentation

PowerPoint training guides are available for Virtual Contact Center Central, Agent Handling, and Basic Scripting. These documents will be provided to you by your CCS Implementation PM. These guides may be distributed as appropriate within your organization for State of West Virginia internal training session beyond the training at the initial implementation.

### Context Sensitive Help

Application/context specific help is available within Virtual Contact Center Central, Studio and the agent interface via the Help buttons located at the top right. Click the Help button from within the area of the application you need assistance with to have the specific help file displayed. This feature can be utilized to provide ongoing training.

### Online Help

Extensive online help is available in VCC Central under Support > External Links > Documentation. This feature can be utilized to provide ongoing training.

Nice inContact University https://university.incontact.com/

Additional training on a variety of topics is available for authorized VCC users via the inContact University web site. Your login credentials for VCC can be used to access the resources available here.

- ACD Agent (eLearning): Agent training on VCC Central and agent interface.
- ACD Supervisor (eLearning): Provides managers and supervisors an overview of the key features related to Agent Call Monitoring. Additional training is available on a number of topics. Below are some additional recommendations for VCC Administrators, Managers, and Supervisors.
- Dashboard Fundamentals (eLearning): Provides an overview of adding, modifying, and deleting widgets and dashboards in Central.
- Reporting Overview (eLearning): Provides an overview of the types of reports that are available within Virtual Contact Center.

  Any State training and documentation requirements beyond the training and documentation offered as described above, will be evaluated for effort and will utilize the Professional Services Fees pricing model.

*4.2.2. Mandatory Project Requirements*

*The following mandatory requirements relate to the goals and objectives and must be met by the Vendor as a part of its submitted proposal.*

*Vendor should describe how it will comply with the mandatory requirements and include any areas where its proposed solution exceeds the mandatory requirement.*

*Failure to comply with mandatory requirements will lead to disqualification, but the approach/methodology that the vendor uses to comply, and areas where the mandatory requfrements are exceeded, will be included in technical scores where appropriate.*

*The mandatory project requirements are listed below.*

## Verizon Response

Verizon has read and understands.

*4.2.2.1 Managed Voice Services*

*4.2.2.1.1 The Vendor must provide a turnkey technical support solution that ensures the continued operations and MACD needs of the State's existing telephony infrastructure, as defined in Appendix A, through the migration period to a Hosted VoIP solution. Additionally, the Vendor must, at the State's discretion, migrate any site to the hosted solution.*

## Verizon Response

Verizon has read and understands.

*4.2.2.2 Hosted Voice Services*

*4.2.2.2.1 The Vendor must agree the State owns all data gathered under the scope of this contract and the Vendor must produce and/or return the data upon the State's request in an editable format.*

## Verizon Response

Verizon has read and complies.

*4.2.2.2.2 Vendor's solution must provide support for local failover and/or survivability services, if requested by Agency, in the event the hosted service becomes inaccessible.*

## Verizon Response

Verizon has read and complies.

Verizon has addressed failover and survivability in the solution section of the response and will recommend SRST as needed for the critical sites upon further discovery/design.

*4.2.2.2.3 Vendor's solution must provide local telephone numbers in West Virginia.*

## Verizon Response

Verizon has read and complies.

Service availability will be checked prior to design for each location desiring service. Additionally, Hosted Voice with local PSTN handoff can be provided for any location where Verizon local service is not available using that location's Cisco router.

*4.2.2.2.4 Vendor's solution must support inbound Automatic Number Identification (ANI).*

### Verizon Response

Verizon has read and complies.

*4.2.2.2.5 Vendor's solution must include inbound Caller ID, outbound custom telephone number, and outbound custom name display.*

### Verizon Response

Verizon has read and complies.

*4.2.2.2.6 Vendor 's solution must support Dialed Number Information Services (DNIS) on 800 # toll-free telephone services.*

### Verizon Response

Verizon has read and complies.

*4.2.2.2.7 Vendor's solution must support rerouting of calls to an alternate site at the State's directive.*

### Verizon Response

Verizon has read and complies.

The VEC VOIP Administrative portal allows for the forwarding of calls.

*4.2.2.2.8 Vendor's solution must support 900/976 blocking.*

### Verizon Response

Verizon has read and complies.

*4.2.2.2.9 Vendor's solution must support x 11 services (currently 211, 411, 511, 611, 811, 911).*

### Verizon Response

Verizon has read and complies.

*4.2.2.2.10 Vendor's solution must include Direct Inward Dial (DID) feature and service.*

### Verizon Response

Verizon has read and complies.

DIDs are available and billable as single numbers on the Verizon platform. DIDs no longer need to be purchased in blocks of 20 so a single DID is reflected as 1/20 of the price on the cost sheet.

*4.2.2.2.11 Vendor's solution must support Operator services.*

### Verizon Response

Verizon has read and complies.

*4.2.2.2.12 Vendor's solution must support local number portability.*

### Verizon Response

Verizon has read and complies.

Verizon will confirm number portability per site upon service validation and coverage.

*4.2.2.2.13 Vendor's solution must provide unlimited free local and long-distance calling.*

### Verizon Response

Verizon has read and complies.

*4.2.2.2.14 Vendor's hosting center(s) must be located within the continental United States.*

### Verizon Response

Verizon has read and complies.

Verizon has two geo-redundant data centers for each Hosted Voice platform.

*4.2.2.2.15 Vendor must provide Train the Trainer sessions for Hosted Voice Services implementations.*

### Verizon Response

**Standard/High Security Hosted Voice and Virtual Communications Express Training:**

There are three options for Hosted Voice services training.

One is that OT can provide end user phone training and any additional Administrative portal training the State may require if opting not to use the online instructor led Administrative scheduled classes.

Second option is that Verizon can provide “Train the Trainer” training, and those trainers will train the end users.

Third, Verizon will provide end user phone training.

Verizon’s training would be web based or custom on site requested training via Professional service rates is available and can be referenced on the cost sheet. Verizon CTD houses up-to-date user guides in the library section, to include how to use the phones selected by the State.

The Customer Training and Development (CTD) web site is https://customertraining.verizon.com/ ).

CTD utilizes Instructor Led Training via Live Meeting and Audio Bridge Registration is required, but there is no charge to access the web site once registered. The VEC/CTD portal provides solution specific documentation that can be utilized for ongoing training and supplement the State’s LMS.

### Verizon Enterprise Center

The Verizon Enterprise Center (https://enterprisecenter.verizon.com/ ) offers a suite of web-based applications that allows you to streamline business processes and control critical business functions, while having 24x7x365 access to a virtual communications center.

Through applications on the Verizon Enterprise Center, you are empowered with the ability to view, track, and customize the products that help you to run your business.

The Verizon Enterprise Center Portal also contains a comprehensive list of services and products and telephone numbers for all key Verizon points of contact.

The Hosted Voice administrative users guide for the administrative portal is available here: https://customertraining.verizon.com/commercial/ug_uccaas_index.htm .

### Verizon Enterprise Center Registration

It is important to register for your Verizon Enterprise Center access promptly so it is available when needed. Please remember to keep your log in information accessible and secure.

Your Account Team can guide you through the following enrollment process:

Step 1. Your Account Team will verify your contract details. They may need to submit an entitlement request for you, since the Managed Services Portal—ESP entitlement will be required for access to Performance Management Reports when available, as well as ESP short codes.

Step 2. You will then self-register on the Verizon Enterprise Center by following the prompts.

Step 3. The Verizon Enterprise Center will email you a verification code, confirming registration.

Step 4. You will use that verification code to complete the self-registration.

Step 5. Inform your Verizon Account Team you've successfully registered and that your Portal access should be enabled.

Step 6. Your Account Team will notify the Service Management team to enable your Portal access.

To register a user account on the CTD website:

Step 1. Go to https://customertraining.verizon.com/

Step 2. Select the appropriate category: Commercial.

Step 3. Click on HOW TO REGISTER and follow the prompts.

Step 4. Follow the prompts to watch the six-minute automated TRAINING ORIENTATION.

To enroll in a class:

Step 1. Login at https://customertraining.verizon.com/

Step 2. Enter the login name and password you created.

Step 3. Click the EVENT LIST link on the left side of the screen.

Step 4. Select the appropriate category.

Step 5. Find the class name and click the ENROLL link.

Click the USER GUIDES/DOWNLOADS link on the left side of the screen to print user guides or reference material.

On the day of the class:

Step 1. Login at https://customertraining.verizon.com/

Step 2. Click on MY SCHEDULE to see your list of enrolled courses.

Step 3. Click the ATTEND link next to the class in which you enrolled.

Step 4: Call the audio bridge that pops up on your screen.

If you have questions or problems, please contact the CTD team:

- CTD telephone: +1 800 662 1049
- CTD website: Step 1. Login at https://customertraining.verizon.com/
- CTD e-mail: ctd-cos@one.verizon.com

*4.2.2.2.16 The State recognizes the need for the inclusion of certain fees and charges mandated by the federal government or Public Service Commission, including but not limited to, Universal Service Fund Fees and 911 Fees.*

*As such, the Vendor must include the latest published version of such fees with its cost response. The State will allow for quarterly Change Orders to care for changes in these fees.*

## Verizon Response

The FCC has issued (6-2006) an interim order that establishes an obligation for providers of interconnected VoIP services to contribute to the Federal Universal Service Fund (FUSF.)

Under FCC rules, interconnected VoIP services are defined as IP-enabled services that

(1) Enable real-time, two-way voice communications;

(2) Require a broadband connection from the users location;

(3) Require IP-compatible customer premises equipment; and

(4) Permit users to receive calls from and terminate calls to the PSTN.

This fee will not apply to any equipment charges associated with VoIP service. Further details can be found on the Federal Communications Commission website at http://www.fcc.gov/.

The taxes and surcharges provided are for informational purposes only and if the tax and/or surcharge amounts change prior to the issuance of the invoice, the customer will be responsible for the taxes and surcharges stated on its invoice even if the taxes and surcharges are different than those shown.

Verizon applies taxes and surcharges in accordance with applicable law, and therefore, such taxes/surcharges are subject to change.

*4.2.2.3 Hosted Contact Center Services*

*Vendor's Contact Center solution must support:*

*4.2.2.3.1 Automatic Call Distributor (ACD)*

### Verizon Response

Routing of an inbound contact may have several factors that can be utilized in determining how and where a contact is to be delivered to the best possible target. Factors external to VCC (DNIS and ANI) are two initial factors.

Once inside VCC, the contact may be analyzed by factors that are incorporated into the routing scheme that was configured in Studio based on factors generated by conditions within VCC (all agents busy, heavy call volume, SLAs, etc.) or other factors that are obtained through integration with other 3rd party sources (most favored client as identified by DNIS, ANI, caller entered data gathered along the routing path), and the availability of the best skilled agent at that moment across any channel.

VCC offers sophisticated skills-based routing. Every agent can be assigned one or more skills, and for each skill assignment the agent can be configured to a specific proficiency level. An incoming call is then routed to the next available agent with the highest proficiency—regardless of their physical location.

If there are multiple available agents with the same proficiency, the call is delivered to the agent who has been available the longest. This technique ensures that callers are routed to the most qualified, available agent.

A lower proficiency could also be used to manage back-up agents for a queue. For example, a supervisor would be very qualified to handle a call, but generally he/she would not be taking calls unless there was high call volume or a shortage of agents.

Another advanced feature bundled with skill-based routing is priority routing. In some circumstances it is helpful to identify high-priority calls and to move them to the front of the queue.

Once you've identified a high-priority caller, through the use of a special toll-free number or a data dip, VCC makes it simple to handle that caller next even if there is a queue of other callers waiting to speak to an agent.

*4.2.2.3.2 Computer telephony integration (CTI)*

### Verizon Response

Computer Telephony Integration can mean many things to different people. To some, it could mean a screen pop to an agent. To others, it could mean integration of telephony data with external data sources.

However you view CTI, it's easy to see it as a means to an end. VCC's CTI capabilities help you provide a personalized service experience that your customers that enhances the overall customer journey.

Our cloud-based call center platform identifies your customers by unique identifiers, such as their phone number or account number, and once identified, back-end CTI can provide them with information that's helpful and relevant to them. Information like a local address, account balance, or even local power outage information.

And, if the customer needs to then talk to an agent, the VCC platform determines the right agent queue to handle the inquiry and/or the priority of that particular caller. Once the correct agent has been identified by the system, desktop CTI is used to "pop" the right customer screen.

This reduces call handle time and leads to increased customer bliss, which of course, means more business for you.

Additionally, as part of the CTI solution, VCC also offers desktop CTI that enables your agents' call control interface to be completely embedded within browser-based CRMs like Salesforce.com (among other CRMs and databases).

This merges your technologies, creating a seamless flow of information that provides customers the answers they need fast and gives agents easy access to the information they need to deliver a superior service experience including the ability to dial directly from the agent CRM/DB application through consumption of NICE inContact APIs.

*4.2.2.3.3 Call control*

### Verizon Response

All contacts will traverse and remain within the VCC cloud based system for the duration of the contact.

Therefore all telephony controls needed by the agent will be utilized within the agent user interface (outbound dialing, transfer, conference, etc.) The VCC cloud based system will control all contact media (voice, email, chat, etc.).

*4.2.2.3.4 E.164*

### Verizon Response

VCC uses the E.164 format with a leading '+' for numbering in all of our call switching facilities for SIP trunking.

*4.2.2.3.5 Interactive voice response (IVR)*

## Verizon Response

VCC delivers a comprehensive, flexible IVR solution that is unified with the ACD. VCC has the ability to identify callers by unique attributes, like phone number or other customer provided information for self-service or intelligent routing and then display that information, such as the caller's name, on the agent's screen when the call is connected.

To increase agent proficiency and minimize average handle time (AHT), VCC can help facilitate computer telephony integration (CTI) with systems of record like customer relationship management (CRM) systems through the use of database connections (ODBC) or web services (RESTful and SOAP).

This provides features like an immediate screen pop of the customer (if routed to an agent) / caller's record to the agent when the call begins and memorializing caller activity and other IVR data back into the system of record upon call completion.

VCC has the ability to create automated customer interactions (self-service IVR), saving time and money by offloading routine activities that do not require agent intervention; thus allowing agents to be more readily available to assist callers for technical and in-depth questions.

VCC's self-service applications often employ the use of text–to-speech to provide 24x7x365 access to information needed by your callers. Our IVR can extract variable information from a database, or from the web, and convert it to audible speech.

By responding to prompts provided by the IVR system, callers can receive any available text found in an organizations' database in the form of a speech to text or recorded prompt delivery.

The IVR Speech Recognition capabilities allows callers to use voice prompts in conjunction with their own voice, instead of the phone pad, to interact and get access to a wide host of information.

Instead of listening to long menus and pressing on phone pad buttons to choose the desired service, the user can simply say the service's name, and the IVR will connect the user to their desired destination.

Through this use of a voice interface, callers can complete simple tasks quickly; also providing callers with a hands-free experience while navigating the IVR. Speech recognition by greatly reduces the steps a customer takes to accomplish a task, and also increase his satisfaction in the process.

The VCC IVR provides (but not limited to) the following:

- Provide menu options for callers in both touch tone and directed speech recognition
- Query a database or multiple databases for information or intelligent routing and self-service capabilities
- Dynamic IVR menu prompting and data-directed routing
- Survey capabilities
- Read Text-to-Speech back from database driven interactions to callers

- Support for language prompts across any language
- Managed or controlled transfers
- Flexible recording rules, including recording of the contact from system/caller side or entire conversation

VCC will use our expertise to provide consultative support to help you define the best IVR methodology to support your requirements, no matter how complex.

*4.2.2.3.6 Voice Recording*

### Verizon Response

VCC Studio has a Prompt Recorder that can be used to record prompts over the phone. If State of West Virginia currently has a professional recording studio where recordings are created, recorded .wav files can be uploaded to VCC for use by call routing scripts.

*4.2.2.3.7 High Availability with load balancing and built-in redundancy*

### Verizon Response

VCC utilizing NICE inContact builds disaster recovery and high availability (HA) capabilities into its data centers and software. NICE inContact requires multiple sets of redundant services, systems, and hardware.

All systems are monitored at multiple levels including environmental, hardware and application and all monitoring is fed back to the inContact Network Operations Center. Additionally, applications are designed to allow for automatic recovery and fail over of services.

VCCs skills-based, hosted, all-in-one solution turns traditional load balancing technology into "antiquated" technology. VCC views all agents across a customer's business unit (an individual VCC tenant) as a single resource pool.

As a result it isn't necessary to have a "special" premise tool to look into individual call centers and determine if agents are available in one location versus another. VCC routes contacts to the next agent regardless of where that agent is physically located.

In addition, VCC can provide a series of fallback positions where agents having varied skill sets can be brought in to support service level needs.

For example, one of VCC's customers has trained every employee to provide general customer service calls but prefers that specialists normally process calls. When call spikes occur, the secondary "general customer service" skill is engaged and anyone in their facility can be engaged to provide customer service.

*4.2.2.3.8 Vendor must provide Train the Trainer sessions, encompassing all Hosted Contact Center roles - Administrator, Supervisor, and Agents.*

## Verizon Response

VCC and NICE inContact developed a hands-on education program for our customers. Whether you are a supervisor, agent, or an administrator, VCC has an education program that can help you master our call center software solutions and maximize their full potential.

We've developed a number of flexible education offerings for you to choose from when considering your training objectives.

Our education solutions include:

- Instructor-Led Virtual Education: In today's busy world, it's not always possible to leave the office. Enjoy the personal connection of instructor-led education without leaving your desk via web conference.
- Self-Paced eLearning: Students can also take education at their own pace, on their own schedule with our Internet-based eLearning solution.

Training is provided by VCC and optionally by NICE inContact trainers. VCC and NICE inContact also offers a train the trainer learning approach based on your specific needs.

*4.2.2.4 Security*

*4.2.2.4.1 The proposed solution must adhere to the security and privacy baseline standards in accordance to the high-security and standard-security use-case requirements.*

## Verizon Response

Verizon has read and understands.

*4.2.2.4.2 Must adhere to the State of West Virginia's Cyber Security & Privacy policies, procedures, and standards; these can be viewed at the following link: http s://technolog .wv.gov/securit v/Pa !.!es/policies-issued-b -the- cto.aspx*

## Verizon Response

Verizon has read and understands.

*4.2.2.4.3 Must adhere to all applicable security and privacy standards and provide compliance for components and network segments that are subject to the following:*

- *Health Insurance Portability and Accountability Act (HIPAA) requirements as outlined in the attached Business Associate Addendum (BAA);*
- *Federal Information Security Management Act (FISMA), National Institute of Standards Technology's Special Publication (NIST SP) 800-53, NIST SP 800-17 which serve as the baseline;*
- *Family Education Rights and Privacy Act (FERPA) requirements;*
- *Criminal Justice Information System (CHS) requirements;*
- *Payment Card Industry Data Security Standards (PCI-DSS) requirements;*

- *Federal tax Information (FTI) and Internal Revenue Service publication 1075 (IRS 1075) requirements;*
- *Centers for Medicare & Medicaid (CMS) Services Information Security Policy requirements.*
- *Ensure network boundary and access control protection such as dual session boundary controllers and firewalls.*
- *Data-at-rest and data-in-transit encryption.*
- *Role-based access control for all applications which process and/or store sensitive data, to ensure need-to-know policies are enforceable.*

## Verizon Response

The Standard Security Hosted Voice solution may be used in the Healthcare industry in situations where customers are subject to HIPAA.

To the extent the customer and Verizon have signed a Business Associate Agreement (BAA) describing the party's respective responsibilities regarding the use of this solution in a HIPAA-ready healthcare environment, and customer specific solution requiring HIPAA would exclude the following capabilities:

- Telephony recording (e.g., of conversations), other than voice messages
- Video recording
- Speech or voicemail conversion to text
- Voice Message backup
- Forwarding of Voice Message .wav files from the data center

Customers requiring HIPAA solutions must agree to support the following capabilities:

- Integration of Hosted Voice applications to it LDAP/Active Directory for authorized users and for user name and password validation
- Customer administration of voicemail PIN changes

UCCaaS High Security Hosted Voice (Unified Communication and Collaboration as a Service) for Government is FedRAMP (The Federal Risk and Authorization Program) compliant.

FedRAMP processes are designed to assist federal government agencies in meeting Federal Information Security Management Act (FISMA) requirements for cloud systems. The solution is FIPS 140-2 Compliant and all other Federal standards of certification can be viewed in the below matrix.

| # | Question | Response |
|---|---|---|
| 1 | Does the High Security Hosted Voice Federal solution meet HIPAA security Requirements? | We have not yet evaluated HIPAA compliance. |
| 2 | Does the High Security Hosted Voice Federal solution meet FISMA security Requirements? | FISMA is more oriented towards a private cloud, and is not applicable to the High Security Hosted Voice Federal solution. |
| 3 | Does the High Security Hosted Voice Federal solution meet Family Education Rights and Privacy Act (FERPA) security Requirements? | We have not yet evaluated FERPA compliance. |

| # | Question | Response |
|---|---|---|
| 4 | Does the High Security Hosted Voice Federal solution meet CJIS security requirements? | We have not yet evaluated CJIS compliance. |
| 5 | Does the High Security Hosted Voice Federal solution meet the Federal tax information (FTI) and IRS Service publication 1075? | We have not yet evaluated FTI or IRS requirements. |
| 6 | Does the High Security Hosted Voice Federal solution meet the Medicaid and Medicare (CMS) Services Information Security Policy requirements? | We have not yet evaluated Medicaid and Medicare (CMS) security requirements. |
| 7 | Does the High Security Hosted Voice Federal solution meet the Payment Card Industry Data Security Standards (PCI-DSS)? | We have not yet evaluated PCI-DSS security requirements. |
| 8 | Does the High Security Hosted Voice Federal solution ensure network boundary and access control protection, such as dual session boundary controllers and firewalls? | The High Security Hosted Voice network boundary and access control protection is documented in our SSP package and meets FedRAMP compliance requirements, along with being audited annually by a third party assessment organization. |
| 9 | Does the High Security Hosted Voice Federal solution ensure that data-at-rest and data-in-transit are encrypted? | Data-at-rest and data-in-transit meet FedRAMP compliance requirements and are documented in our SSP package, along with being audited annually by a third party assessment organization. |
| 10 | Does the High Security Hosted Voice Federal solution High Security Hosted Voice incorporate role-based access control for all applications which process and/or store sensitive data to ensure need-to-know policies are enforceable? | Role-based access control (RBAC) in the High Security Hosted Voice Federal solution meets FedRAMP compliance requirements and is documented in our SSP package, along with being audited annually by a third party assessment organization. |

The Federal Risk and Authorization Management Program, or FedRAMP, is a program by which the U.S. federal government determines whether cloud products and services are secure enough to be used by federal agencies. FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. Cisco FedRAMP-authorized solutions provide strong, risk-based security that meets federal standards. FedRAMP authorization means that cloud offerings meet the federal government's stringent requirements, as verified by a third party. You can implement Cisco FedRAMP-authorized solutions with full confidence in their security. The Verizon UCCaaS FedRAMP offering is HCS-G FedRamp Moderate Compliant. Below is the link to the GSA website the Cisco Hosted Collaboration Solution for Government (HCS-G) as a federally approved platform.
https://marketplace.fedramp.gov/#/products?sort=productName

- VCC – Please see the attached Verizon Virtual Contact Center Powered by NICE inContact Security documents provided in Appendix C of this proposal.
- VCE- Please see the attached Verizon Virtual Communications Express BroadSoft/Cisco Security document provided in Appendix D of this proposal.

*4.2.2.4.4 Vendor must draft a cyber risk management plan outlining the process, by which, cyber risk management activities are conducted to identify, assess, communicate, and manage shared cyber risk. The Vendor must provide this prior to the first implementation on the Vendor's hosted solution.*

### Verizon Response

Verizon has read and understands.

*4.2.2.4.5 Vendor must draft an incident management plan aligned with NIST SP 800-61rev2, whereas both the State and Vendor must mutually approve. The plan must include the outlined scope, responsibility matrix, communications plan, procedures, and deliverables associated with cyber security incident response.*

*In addition, the plan must outline incident reporting requirements, semiannual security reports, and cyber threat intelligence sharing. The Vendor must provide this prior to the first implementation on the Vendor's hosted solution.*

### Verizon Response

Verizon has read and understands.

*4.2.2.4.6 The Vendor must adhere to personnel security requirements for background checks in accordance with state law. The vendor is liable for all costs associated with ensuring staff meets all requirements.*

### Verizon Response

Verizon has read and understands.

*4.2.2.4.7 Vendor must agree to drafting an audit management plan designed to assist the state with conducting internal and external compliance audits when the vendor-supplied solution is within the audit scope. At minimum, the plan must include:*

- *How the vendor will provide a NIST 800-53 security controls report, outlining organizational responsibilities (State, Vendor, or Shared), per each applicable control for each major application/information system within the audit scope.*
- *Plan of Action & Milestone documentation for non-compliant security & privacy controls when the vendor holds primary or shared control responsibility.*

*The Vendor must provide this prior to the first implementation on the Vendor's hosted solution.*

### Verizon Response

Verizon has read and understands.

*4.2.2.5 Service and Support*

*4.2.2.5.1 Vendor must provide a network operation support center(s) for all tiers of support, including end-user support, that is available 24x7x365 and is accessible via a toll-free number.*

## Verizon Response

The Verizon MNSO NOC provides Tier 1-3 support.

Verizon will also be providing a 24x7x365 user help desk for all services proposed.

*4.2.2.5.2 The successful Vendor must assign an experienced and skilled Project Manager who will provide a high-level project management plan including key components such as a project charter, issue tracking, statements of work (SOW), work breakdown structures (WBS), implementation schedules, etc. in accordance with the Project Management Body of Knowledge (PMBOK) or other industry standard project management methodology stated in West Virginia State Code (§5A-6-4b).*

*The link can be found at: http://www.legis.state.wv.us/WVCODE/Code.cfm?cha p=05a&art=6#06.*

*The project management plan must be submitted to and approved by the WVOT Project Management Office (PMO) prior to engaging the first agency for VoIP services implementation.*

## Verizon Response

Verizon has read and understands.

*4.2.2.5.3 The successful Vendor's Project Manager must track and report (via written status reports) the following: schedule, scope, budget, issues, risks, specified performance indicators, and other metrics determined appropriate throughout the project and each site implementation.*

## Verizon Response

Verizon has read and understands.

*4.2.2.5.4 Vendor must work with the WVOT using the established Telecommunications Change Request (TCR) procedures for ordering and implementing these telecommunications services.*

## Verizon Response

Verizon has read and understands.

*4.2.2.5.5 Vendor billing errors must be credited back to the State from the effective date of the error. The State reserves the right to withhold payment until credit is received.*

## Verizon Response

Verizon has read and understood and would like to add the following language to clarify billing disputes.

"In the event that Customer reasonably determines that there is a material discrepancy between Verizon's invoiced charges and Customer's calculation of charges owed, Customer may withhold only the Disputed amount of the invoice.

A "Disputed" amount is one for which Customer has given Verizon written notice, adequately supported by bona fide explanation and documentation. Any invoiced amount not Disputed within 6 months of the invoice date is deemed correct and binding on Customer.

Verizon will make every commercially reasonable effort to resolve Disputed amount within 60 days after receiving Customer's notice, but cannot guarantee that."

*4.2.2.5.6 For auditing, billing, and support purposes, the State requires any service with an associated rate to be identified on its monthly bill. As such, the State must be provided, at a minimum, the following:*

- *Billing Month*
- *Billed Entity Name*
- *Customer Name/Account (if different from billed entity)*
- *Service Location*
- *Service Period*
- *Itemized Cost for Individual Billing Components*
- *Itemized Call Detail*
- *Itemized Cost for Any One-Time or Non-Recurring Charges*
- *Itemized Cost for Any Surcharges and Total Cost*

*The cost identified in the bill must match the contract rates for the specified services. The Vendor must provide the State's monthly bill in an editable format such as Excel and/or csv.*

### Verizon Response

Verizon's invoice will be presented both in hard copy via mail and in PDF format. The invoice will not be presented in an editable format such as Excel and/or csv. However, Verizon can provide reports in a text or csv format which can be exported to Excel.

*4.2.2.5.7 The Vendor must invoice on a consistent monthly billing cycle across all services. Services installed or disconnected for a partial month must be prorated based on the date the service is activated/accepted or disconnected.*

*The Vendor must not bill the State of services until the services have been activated and accepted as functional. The Vendor shall not bill the State for services after the disconnect due date listed on the submitted TCR.*

### Verizon Response

Verizon has read, understood and agrees to comply.

*4.2.2.5.8 The Vendor must provide and update a weekly status report and/or order log for submitted TCRs.*

### Verizon Response

Verizon has read and understands.

*4.2.2.5.9 If, as part of its proposal, the Vendor submits appendices or other supplemental materials, the Vendor must denote specifically in those materials where the relevant information is located.*

### Verizon Response

Verizon has read and understands.

*4.2.2.5.10 The State expects full, complete, and timely cooperation in disentangling the relationship in the event that the Agreement expires or terminates for any reason.*

*In the event of expiration or termination, the State expects that the Vendor shall, among other things: return all State data and documentation to the State, including but not limited to configuration information; transfer ownership of all leased equipment at no cost to the State (other than the payments already received by the Vendor under the Agreement); and, allow the State or the replacement provider(s) continued access to all billing, ordering, and trouble ticketing systems, and processes that have been employed in servicing the State, in accordance with methods and procedures to be agreed upon and established in the Agreement. Please acknowledge your acceptance of this.*

### Verizon Response

Verizon agrees to full, complete, and timely cooperation in disentangling the relationship in the event that the Agreement expires or terminates for any reason.

Verizon agrees to negotiate in good faith with regard to transfer of ownership of all leased equipment.

## 4.3. Qualifications and Experience

*Vendor should provide information and documentation regarding its qualifications and experience in providing services or solving problems similar to those requested in this RFP. Information and documentation should include, but is not limited to, copies of any staff certifications or degrees applicable to this project, proposed staffing plans, descriptions of past projects completed (descriptions should include the location of the project, project manager name and contact information, type of project, and what the project goals and objectives where and how they were met.), references for prior projects, and any other information that vendor deems relevant to the items identified as desirable or mandatory below.*

*4.3.1. Vendor should describe in its proposal how it meets the desirable qualification and experience requirements listed below.*

*4.3.1.1. Vendor should provide three (3) examples demonstrating at least three (3) years of experience in providing a Hosted VoIP solution of a similar size and scope - 15,000 users across 200 sites with one example being a public entity.*

*Vendor should provide a summarization of each project including goals and objectives, total number of phones deployed per site, length of time deployment took, if still in service, and reference for each example.*

### Verizon Response

**Commonwealth of Massachusetts Health and Human Services**

- Contact: Beth Beard, IT Director

- Contact Phone: 617-216-3580
- Contact Email: beth.beard@state.ma.us

The project converted 20,000 users, across 150 locations in 2013 to Verizon's Hosted UCCaaS solution, over a 13 month installation timeframe. Services are still in place. Much like the State of WV their goals/objectives were to transition to a Hosted solution OP EX vs CAP EX.

As a requirement to use this reference the State of WV must contact Sandra Hawkins on 304-356-3395 before contacting Beth Beard and allow time for our Account Manager from Commonwealth of Massachusetts to notify Beth to expect a call from State of West Virginia.

### CALNET

The State of California under "CALNET" contract has transitioned 60,356 user, across 743 locations to a Hosted VoIP solution. The contract was awarded to Verizon 2007.

The largest agency in the State of California to transition to Hosted VoIP is the Employment Development Department (EDD)

- Contact: Robert Delaney, IT Supervisor II, Voice Operations, Production Services Division
- Contact Phone: 916-653-8756
- Contact Email: robert.delaney@edd.ca.gov

Goal/objectives were to establish an IP based service offering for voice, video, and data services, providing a migration path to convergence for cost savings.

### Commonwealth of Pennsylvania

The Commonwealth of Pennsylvania contract has transitioned 42,000 user, across 225 locations to a Hosted VoIP solution. The transition occurred during 2012.

- Contact: LaRae Allen, Supplier Manager
- Contact Phone: 717-772-8009
- Contact Email: larallen@pa.gov

As a courtesy to our customer please contact Sandra Hawkins (304)356-3395 or Tonya Fazio (717)777-8520 to coordinate contact with Commonwealth of Pennsylvania. The goals of this project were to support the Commonwealth's needs to implement the hosted VoIP solution to transform from a TDM Centrex voice environment to one that would enable them to collaborate and operate more effectively. The hosted model provided the solution "as a service" with responsibility for management and support from Verizon, rather than customer resources.

### Convestro NV

Convestro has transitioned 17,000 user, across 60 locations to a Hosted VoIP solution. The transition occurred over three years ago, took 10 weeks to deploy, and is still in service today.

- Contact: Eric Brouwers, ISE Infrastructure Services
- Contact Phone: +32 3 540 3906
- Contact Email: eric.brouwers@covestro.com

*4.3.1.2. Vendor should provide at least one (1) example demonstrating at least three (3) years of experience in providing single/multiple Hosted Call Center solutions of a similar size and scope - 500 users across 20 sites.*

*Vendor should provide a summarization the project including goals and objectives, total number of agents per site, length of time deployment took, if still in service, and reference for the example.*

## Verizon Response

### State of California (CALNET 3)

Under CALNET 3 (State of California Technology contract) Verizon currently has over 3400 agents on a hosted contact center platform, across 57 contact centers, and close to 100 sites. Customers range from school districts, to Higher Ed customers, to City of LA to small and large state agencies. The complexity of the contact centers vary widely. Calnet3 customers have been on the platform as long as April, 2013 with new customers coming on board every month. A typical implementation is 45 to 60 business days and another 30 to 60 days should be added for complex integrations or advanced features. Large complex contact centers can take from 9 months to a year. Small contact centers can be quicker, if the agency knows what they want or can quickly make decisions. Verizon has put contact centers in place very quickly when needed, even as quick as 1 week from order to go live.

There is not one single contact for the CALNET contact center services however California Employment Development Department (EDD) will be happy to answer questions and serve as a reference. EDD has 3 main call centers Tax, Disability Insurance and Unemployment Insurance. They have been a Verizon Call Center customer for over 10 years with VCC being installed in November 2014 and March 2015. Their call volume varies from a high of 21M calls/month (Sept 2013) to 700K calls/month (current rate with unemployment low). Having a system that can handle their fluctuations, offer 24X7 services, and has strong reliability as measured in up time are some of their key goals and objectives.

- Contact: Maria Bonilla, Chief, Telecommunications Section
- Contact Phone: 916-654-7875
- Contact Email: maria.bonilla@edd.ca.gov

*4.3.1.3 The State desires an Account Team (including Account Support Representative, Technical Support Representative, Solution Implementation Support Representative, Contract Manager, Billing Support Representative, Security/Compliance Specialist, and Project Manager) for the winning solution and life of the contract.*

*Vendor should describe in detail the responsibilities of key roles and staff's experience in working in these roles.*

## Verizon Response

Please reference the Account Service Plan provided in Appendix I of this proposal.

*4.3.1.4 Vendor should describe its experience and process in conducting cyber risk management ensuring shared risk is identified, assessed, communicated, and managed.*

## Verizon Response

Please reference the Cyber Security Program documentation provided in Appendix E of this proposal.

VCC - NICE inContact's network is designed around carrier and enterprise grade technology for its switches, routers, firewalls and telecom devices. All network equipment is designed for high availability, fault tolerance, redundancy, and scalability.

The NICE inContact Network Operations Center (NOC) continuously monitors all traffic (including entry and exit points) 24x7x365. All systems are monitored at multiple levels including environmental, hardware and application.

The NOC is first to receive notifications/alarms about system or service issues. All events, incidents, and disasters are monitored, managed, escalated and communicated through this Network Operations Center located in Salt Lake City, UT.

Verizon does have policies and procedures that ensure prompt notification of customers in the event of an incident, as well as procedures to address necessary remediation. Customer notification groups are configured and communications are sent out via email.

*4.3.1.5 Vendor should describe its experience and process for conducting NIST SP 800- 53 security assessment and authorization control families' activities, designed to ensure each vendor-provided solution implementation adheres to security and privacy requirements before being placed into production.*

## Verizon Response

Verizon's BSA provides an assessment of your information security program maturity relative to any number or individual, or combined, industry accepted security program frameworks.

Verizon uses the selected standard(s) to review the security program relative to the Scope, Performance, and Maturity of the Security Program. This BSA uses NIST 800-53.

All BSA's are accomplished the same way using a three phase approach that includes: Phase 1, Project Initiation and Data Collection; Phase 2, Data Analysis; and Phase 3, Review and Reporting.

Verizon will present the results of the BSA as a written report. This report consists of a detailed managerial and operational Report-of-Findings of the security posture of the evaluated people, processes, and technologies. The entire BSA process takes approximately 6-9 weeks depending on your availability.

VCC - Security is taken very seriously utilizing NICE inContact. Security measures include intrusion detection/intrusion protection devices and software, IP screening, port filtering, and other industry standard measures.

Security on applications which customers will have access to will include application password encryption by means of salted hashes, and access links to CXone via https:// and/or SSL. Typically customers use the http:// url and CXone does a redirect to the HTTPS site.

NICE inContact implemented a robust layered security policy on all IP POP elements including but not limiting to:

- User access controls utilize a user/password login, where users are in turn controlled via roles based permissions model that is client administered and configurable.
- Web servers are in firewall secured DMZ's
- IDS/IPS systems monitor intrusion activities and prevent penetration
- Regular vulnerability scans and penetration tests are performed
- Anti-virus is deployed on all systems
- NICE inContact utilizes Sonus SBCs; an SBC is essentially a VoIP firewall
- NICE inContact offers solutions to allow the creation of a 'private' network for VoIP traffic

NICE inContact perform quarterly and yearly audits, a yearly SOC2 report and we obtain assurances such as a 70/SSAE 16 or Vendor Security Questionnaire from all of their facility vendors.

NIST is a framework that describes categories of compliance of cloud providers. As such, we do fit within many of the NIST definitions of public cloud provider categories as a SaaS provider. However, certification within the NIST controls is most often performed within a FedRAMP audited environment.

NICE inContact maintains such a FedRAMP environment as an option.

*4.3.1.6 Vendor should list all government or standards organization security certifications it currently holds that apply specifically to the vendor's proposal, as well as those in process at time of response.*

*Specifically include HIPAA, CMS, FERPA, CJIS Security Policy, PCI Data Security Standards (DSS), IRS Publication 1075, FISMA, NIST 800-53, NIST SP 800-171, and FIPS 200 if they apply.*

## Verizon Response

The Verizon UCCaaS offers flexible bundles of Cisco-powered services, including call control, voicemail, presence, instant messaging, and unified desktop and mobile clients.

The Federal Risk and Authorization Management Program, or FedRAMP, is a program by which the U.S. federal government determines whether cloud products and services are secure enough to be used by federal agencies.

FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

Cisco FedRAMP-authorized solutions provide strong, risk-based security that meets federal standards. FedRAMP authorization means that cloud offerings meet the federal government's stringent requirements, as verified by a third party. You can implement Cisco FedRAMP-authorized solutions with full confidence in their security.

The Verizon UCCaaS FedRAMP offering is HCS-G FedRamp Moderate Compliant. Below is the link to the GSA website the Cisco Hosted Collaboration Solution for Government (HCS-G) as a federally approved platform.

https://marketplace.fedramp.gov/#/products?sort=productName

VCC and High Security VCC (VCC for Government) is HIPAA ready and PCI compliant.

## FISMA

Since VCC is a multitenant platform, VCC for Government is FedRAMP Authorized as opposed to FISMA which is typically used for single tenant systems. Visit FedRamp.Gov for further information. Certifications include: SOC 2 Type 2 audited data centers, PCI compliance, Privacy Shield certification, change control policies, regular and timely security patch management, disaster recovery planning and security training provide regulatory compliance and service integrity.

FISMA is partially built on NIST SP 800-53 and FedRAMP is built on NIST SP 800-53 – so it, as an environment equates to portions of FISMA. FISMA is built on FIPS 199, FIPS 200 and NIST Special Publications 800-53, 800-59 and 800-60. NICE inContact company security framework utilizes SANS and NIST SP800-53. While we don't currently have FISMA compliance certification, many groups use FISMA and FedRAMP interchangeably, even though they are different. We currently can provide a FedRAMP ATO and would welcome further dialogue around security controls and processes to help align to your requirements

## FERPA

VCC and VCC for Governement provides tools for a customer to implement a FERPA compliant contact center. The customer would be responsible to setting the policy and perform the audits to be FERPA complaint. FERPA gives parents certain rights (inspection, correction, and disclosure requirements for granted, stated exceptions) with respect to their children's education records. The VCC product is a service vehicle with which a customer who must be compliant can create a FERPA-compliant solution, but Verizon/Nice/InContact is not bound under the act.

## CJIS

VCC and VCC for Government have access controls, secure encrypted transport, encrypted storage, scans, pen tests, policies, training – etc. to provide West Virginia with a CJIS compliant solution, we do not however audit for CJIS

We perform both an annual PCI DSS level 2 attestations (based on the number of cards expected through our system) and a SOC 2 Type 2 Report for the purposes of confirming security and reliability of our systems. VCC does provide a service environment with PCI level 1 certification if during discovery we determine that an agency requires it. This may incur certain extra charges.

Additionally, all new employees undergo drug and background checks. There is a separation of duties to limit employee access to critical systems and programs / data to the appropriate users and job descriptions. Facilities access is through card controlled entry. Visitors are badged at all times and accompanied while on premise. Regular internal and external audits are performed.

Federal tax Information (FTI) and Internal Revenue Service publication 1075 (IRS 1075) requirements

The Verizon Contact Center solution is certified against standards such as Safe Harbor, CPNI, PCI, SOC 2, SOX 404. There is not an audit specifically against IRS Pub 1075. That being said, we are confident that security controls, in combination with the application of best practices to the design of your contact center solution, will ensure a secure solution that will meet those needs.

FTI is covered in same way as PII -Personally Identifiable Information, PHI -Personal Health Information, etc. This almost always pertains to how we protect call recordings, chat transmissions, data in transit and rest our standard security answers for that topic cover FTI

Centers for Medicare & Medicaid (CMS) Services Information Security Policy requirements.

Per this security standard,CMS-CLD-1 All cloud service implementations must have an approved Federal Risk and Authorization Management Program (FedRAMP) ATO (i.e., FedRAMP Use Case18), Provisional ATO, or an Agency ATO. FedRAMP authorization ensures the minimum baseline controls are in place. Business Owners must verify the CSP meets additional CMS and HHS security, monitoring, and reporting requirements prior to selecting a cloud service. The designated Business Owner must:

- Comply with FedRAMP controls to meet the FedRAMP baseline for the use case under the stated FedRAMP categorization
- Submit an authorization package to the CMS CISO that includes all documentation required by FedRAMP for an ATO and complete all required templates and processes
- Store a redaction of the FedRAMP documentation on the Program Management Office (PMO) website

VCC for Government is FedRAMP authorized. An ATO can be conducted and starts with going to the FedRamp.gov web site to get the security package.

Ensure network boundary and access control protection such as dual session boundary controllers and firewalls

Per the FedRAMP SSP

8.2 INFORMATION SYSTEM COMPONENTS AND BOUNDARIES NICE inContact CXone consists of six divisions as follows:

1. The NICE inContact CXone system boundary. The NICE inContact CXone system components are entirely within the boundary with identified interconnections to the other divisions. The system boundary contains two separate hosting environments:

   a. Amazon Web Services (AWS). Virtualized components reside in fully redundant environments.

   b. Equinix. Voice equipment that cannot be virtualized is hosted in fully redundant environments.

2. The NICE inContact corporate environment. This division does not contain any system components, but certain users access the system from here. This access is provided over a dedicated interconnect that is described later in this document. In addition, there are corporate support and monitoring systems in this environment that receive operational data from within the NICE inContact CXone and surface the information to billing, monitoring, and support systems.

3. External services. NICE inContact CXone makes use of some external services. These are all accessed over the Internet from the AWS environment.

4. The Department/Agency (D/A) network. This division does not contain any system components, but certain users specific to an agency or department access the system from here. This access is provided over a dedicated interconnect that is described later in this document that meets Trusted Internet Connections (TIC) requirements.

5. Public access. Depending on the specific system configuration, public access to nongovernmental tenants may be allowed. In this case, access to the system (excluding government data) may be accessed using web technologies over the Internet. Departments and agencies may choose to leverage this connection if TIC compliance is not required.

6. Patron access. Patrons are individuals that interact with the system through phone calls, email, chat, or other supported communication technologies. Patrons are outside the system boundary and interface with NICE inContact CXone through carriers or other communication providers.

Data-at-rest and data-in-transit encryption.

NICE inContact employs 3PAR Self Encrypting Drive technology that provides FIPS 140-2 encryption for all storage on all its clusters.

We can provide data transport through SFTP which uses encryption in transit with strong (AES 256) encryption and public X.509 certs, etc.

All CXone voice recordings are secured at rest within our Cloud supersite locations. If you should chose to transfer any recordings to their desired storage location, optionally per contract, data can be encrypted while at rest at our EFT (Enhanced File Transfer) terminal. Customer provides their own keys.

Additionally, for VCC for Government data in transit, tenants can collocate routers in a FedRAMP data center (Culpeper/ Miami) for Voice and Data. Otherwise, Data traffic is HTTPS over open Internet to FedRAMP AWS Virtual Path Connection (VPC).

Role-based access control for all applications which process and/or store sensitive data, to ensure need-to-know policies are enforceable.

*NICE inContact: Within the NICE inContact CXone system, data is protected while at rest from unauthorized access, modification, and exfiltration via physical and logical means. Physical access control mechanisms described within this SSP (under security controls PE-3 and PE-6) apply to data resident within facility spaces. Logical mechanisms include role-based access control (RBAC) strong identification and authentication methods, and cryptographic mechanisms that include drive encryption and file encryption. Amazon Web Services (AWS): Several AWS services are used to provide protection of information at rest including AWS S3 and EBS.*

VCC – Please see the attached Verizon Virtual Contact Center Powered by NICE inContact Security documents provided in Appendix C of this proposal.

*4.3.1.7 Vendor should provide a detailed list of the **third-party** attestations, reports, **security credentials** (e.g., Fed.Ramp), and certifications relating to cybersecurity and privacy controls.*

## Verizon Response

VCC – Please see the attached Verizon Virtual Contact Center Powered by NICE inContact Security documents provided in Appendix C of this proposal.

The Verizon UCCaaS offers flexible bundles of Cisco-powered services, including call control, voicemail, presence, instant messaging, and unified desktop and mobile clients.

The Federal Risk and Authorization Management Program, or FedRAMP, is a program by which the U.S. federal government determines whether cloud products and services are secure enough to be used by federal agencies.

FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

Cisco FedRAMP-authorized solutions provide strong, risk-based security that meets federal standards. FedRAMP authorization means that cloud offerings meet the federal government's stringent requirements, as verified by a third party.

You can implement Cisco FedRAMP-authorized solutions with full confidence in their security.

The Verizon UCCaaS FedRAMP offering is HCS-G FedRamp Moderate Compliant. Below is the link to the GSA website the Cisco Hosted Collaboration Solution for Government (HCS-G) as a federally approved platform.

https://marketplace.fedramp.gov/#/products?sort=productName

The Standard Security Hosted Voice solution may be used in the Healthcare industry in situations where customers are subject to HIPPA.

To the extent the customer and Verizon have signed a Business Associate Agreement (BAA) describing the parties respective responsibilities regarding the use of this solution in a HIPAA-ready healthcare environment, and customer specific solution requiring HIPAA would exclude the following capabilities:

- Telephony recording (e.g., of conversations), other than voice messages
- Video recording
- Speech or voicemail conversion to text
- Voice Message backup
- Forwarding of Voice Message .wav files from the data center

Customers requiring HIPAA solutions must agree to support the following capabilities:

- Integration of Hosted Voice applications to it LDAP/Active Directory for authorized users and for user name and password validation
- Customer administration of voicemail PIN changes

*4.3.1.8 Vendor should describe its experience and capabilities in supporting their customers concerning compliance audits when the vendor-supplied solution is within the scope of audit.*

### Verizon Response

Verizon has an internal audit group that is responsible for planning and performing internal audits, independent of compliance certification.

As part of the ISO27001 standard, Verizon needs to conduct regular internal audits across our services. These audits are conducted throughout the year, as they are an ongoing requirement of the ISO27001 standard.

VCC – Please see the attached Verizon Virtual Contact Center Powered by NICE inContact Security documents provided in Appendix C of this proposal.

*4.3.1.9 Vendor should describe its experience and provide an overview of their incident management process and cyber threat intelligence sharing process for incidents associated with the vendor provided solution.*

### Verizon Response

The Enterprise Ticket Management System (ETMS) is the application used by Verizon to manage ongoing incidents. This system is integrated with network monitoring tools.

Approximately 97% of all tickets Managed Networks and Services (MNS) works are pro-active rather than customer initiated.

Verizon's event monitoring tool (SMARTS) uses two methods to detect faults:

- Active Monitoring: Polling (ICMP + SNMP walk): the active monitoring systems are configured to poll any device each 3 minutes.
- Passive Monitoring: SNMP Trap: Devices send an alert each time specific faults occur.

By default, any CPE is configured to send traps for the following faults:

- Each time an interface changes its operational state (up/down).
- Each time a CPE reboots (even if manually reloaded by command).

The ETMS ticket is automatically updated with information from various databases as well as the results from the automated testing performed. ETMS incident tickets can also be accessed by customers from the Verizon Enterprise Center portal.

See Appendix E. Cyber Security Program.

VCC – Please see the attached Verizon Virtual Contact Center Powered by NICE inContact Security documents provided in Appendix C of this proposal.

## 4.4. Oral Presentations

*The Agency will require oral presentations of all Vendors participating in the RFP process. The date of the presentations will be determined at a later time and all vendors will be notified in advance.*

*During oral presentations, Vendors may not alter or add to their submitted proposal, but only clarify information. A description of the materials and information to be presented is provided below:*

*Materials and Information Requested at Oral Presentation:*

*4.4.1. Summary of solution, including product and support offerings, ability to deliver the solution in the specified timeframes, and experience in providing managed and hosted voice solutions.*

*4.4.2. The State will ask clarifying questions regarding the Vendor's submitted technical response.*

*4.4.3. Contact Center Presentation to see a live demonstration of Vendor's offering.*

### Verizon Response

Verizon has read and understands.

# Section 5. Vendor Proposal

## *5.1. Economy of Preparation*

*Proposals should be prepared simply and economically providing a concise description of the items requested in Section 4. Emphasis should be placed on completeness and clarity of the content.*

### Verizon Response

Verizon has read and understands.

## *5.2. Incurring Cost*

*Neither the State nor any of its employees or officers shall be held liable for any expenses incurred by any Vendor responding to this RFP, including but not limited to preparation, delivery, or travel.*

### Verizon Response

Verizon has read and understands.

## *5.3. Proposal Format*

*Vendors should provide responses in the format listed below:*

*5.3.1. Two-Part Submission: Vendors must submit proposals in two received submitted in two distinct parts: technical and cost. Technical proposals must not contain any cost information relating to the project. Cost proposal must contain all cost information and must be sealed in a separate envelope from the technical proposal to facilitate a secondary cost proposal opening.*

*5.3.2. Title Page: State the RFP subject, number, Vendor's name, business address, telephone number, fax number, name of contact person, e-mail address, and Vendor signature and date.*

*5.3.3. Table of Contents: Clearly identify the material by section and page number.*

*5.3.4. Response Reference: Vendor's response should clearly reference how the information provided applies to the RFP request. For example, listing the RFP number and restating the RFP request as a header in the proposal would be considered a clear reference.*

*5.3.5. Proposal Submission: All proposals must be submitted to the Purchasing Division prior to the date and time stipulated in the RFP as the opening date. All submissions must be in accordance with the provisions listed in Section 2: fustructions to Bidders Submittin g Bids.*

### Verizon Response

Verizon has read and understands.

# Section 6. Evaluation and Award

## *6.1. Evaluation Process*

*Proposals will be evaluated in two parts by a committee of three (3) or more individuals. The first evaluation will be of the technical proposal and the second is an evaluation of the cost proposal.*

*The Vendor who demonstrates that it meets all of the mandatory specifications required, attains the minimum acceptable score and attains the highest overall point score of all Vendors shall be awarded the contract.*

### Verizon Response

Verizon has read and understands.

## *6.2. Evaluation Criteria*

***Proposals will be evaluated based on criteria set forth in the solicitation and information contained in the proposals submitted in response to the solicitation.***

*The technical evaluation will be based upon the point allocations designated **below for a** total of 70 of the 100 points. Cost represents 30 of the **100 total points.***

**Evaluation Point Allocation:**

| | |
|---|---|
| Project Goals and Proposed Approach | |
| - Approach & Methodology to Goals/Objectives | 55 Points Possible |
| ○ 4.2.1.1 Voice Services | (40 Points Possible) |
| ○ 4.2.1.2 Security of Solution's Services | (5 Points Possible) |
| ● 4.2.1.3 Service and Support of Hosted Solution | (10 Points Possible) |
| - Approach & Methodology to Compliance with Mandatory Project Requirements | 0 Points Possible |
| Qualifications and experience | |
| - Qualifications and Experience Generally | 10 Points Possible |
| ○ 4.3 Vendor Qualifications and Experience | |
| - Exceeding Mandatory Qualification/Experience Requirements | 0 Points Possible |
| Oral Presentation | 5 Points Possible |
| Total Technical Score: | 70 Points Possible |
| Total Cost Score: | 30 Points Possible |
| Total Proposal Score: | 100 Points Possible |

### Verizon Response

Verizon has read and understands.

## 6.3. Technical Bid Opening

*At the technical bid opening, the Purchasing Division will open and announce the technical proposals received prior to the bid opening deadline. Once opened, the technical proposals will be provided to the Agency evaluation committee for technical evaluation.*

### Verizon Response

Verizon has read and understands.

## 6.4. Technical Evaluation

*The Agency evaluation committee will review the technical proposals, assign points where appropriate, and make a final written recommendation to the Purchasing Division.*

### Verizon Response

Verizon has read and understands.

## 6.5. Proposal Disqualification

*6.5.1. Minimum Acceptable Score ("MAS"): Vendors must score a minimum of 70% (49 points) of the total technical points possible in order to move past the technical evaluation and have their cost proposal evaluated. All vendor proposals not attaining the MAS will be disqualified.*

*6.5.2. Failure to Meet Mandatory Requirement: Vendors must meet or exceed all mandatory requirements in order to move past the technical evaluation and have their cost proposals evaluated. Proposals failing to meet one or more mandatory requirements of the RFP will be disqualified.*

### Verizon Response

Verizon has read and understands.

## 6.6. Cost Bid Opening

*The Purchasing Division will schedule a date and time to publicly open and announce cost proposals after technical evaluation has been completed and the Purchasing Division has approved the technical recommendation of the evaluation committee.*

*All cost bids received will be opened. Cost bids for disqualified proposals will be opened for record keeping purposes only and will not be evaluated or considered. Once opened, the cost proposals will be provided to the Agency evaluation committee for cost evaluation.*

*The Purchasing Division reserves the right to disqualify a proposal based upon deficiencies in the technical proposal even after the cost evaluation.*

### Verizon Response

Verizon has read and understands.

## 6.7. Cost Evaluation

*The Agency evaluation committee will review the cost proposals, assign points in accordance with the cost evaluation formula contained herein and make a final recommendation to the Purchasing Division.*

*Cost Evaluation Formula: Each cost proposal will have points assigned using the following formula for all Vendors not disqualified during the technical evaluation.*

*The lowest cost of all proposals is divided by the cost of the proposal being evaluated to generate a cost score percentage. That percentage is then multiplied by the points attributable to the cost proposal to determine the number of points allocated to the cost proposal being evaluated.*

*Step 1: Lowest Cost of All Proposals I Cost of Proposal Being Evaluated = Cost Score Percentage*

*Step 2: Cost Score Percentage X Points Allocated to Cost Proposal = Total Cost Score*

*Example:*

*Proposal 1 Cost is \$1,000,000*

*Proposal 2 Cost is \$1,100,000*

*Points Allocated to Cost Proposal is 30*

*Proposal 1: Step 1 - \$1,000.000 I \$1,000,000 = Cost Score Percentage of 1 (100%) Step 2 - 1 X 30 = Total Cost Score of 30*

*Proposal 2: Step 1-\$1,000,000 I \$1,100,000 = Cost Score Percentage of 0.909091 (90.9091%) Step 2 - 0.909091 X 30 = Total Cost Score of 27.27273*

### Verizon Response

Verizon has read and understands.

## 6.8. Availability of Information

*Proposal submissions become public and are available for review immediately after opening pursuant to West Virginia Code §SA-3-1 I(h). All other information associated with the RFP, including but not limited to, technical scores and reasons for disqualification, will not be available until after the contract has been awarded pursuant to West Virginia Code of State Rules §148-1-6.3.d.*

### Verizon Response

Verizon has read and understands.

*By signing below, I certify that I have reviewed this Request for Proposal in its entirety; understand the requirements, terms and conditions, and other information contained herein; that I am submitting this proposal for review and consideration; that I am authorized by the bidder to execute this bid or any documents related thereto on bidder's behalf; that I am authorized to bind the bidder in a contractual relationship; and that, to the best of my knowledge, the bidder has properly registered with any State agency that may require registration.*

## Verizon Response

| | |
|---|---|
| Company | Verizon Business Network Services Inc. on behalf of MCI Communications Services, Inc. dba Verizon Business Services |
| Representative Name, Title | Sr Mgr - Billing |
| Contact Phone/Fax Number | Phone: 304-356-3395 \| Fax: N/A |
| Date | November 20, 2018 |

# Appendix A. Overview of Current Telephony Environment

Appendix
A_Overview of Curre

## Verizon Response

Verizon has read and understands.

## *APPENDIX A (revised 10/24/2018)*

## *OVERVIEW OF CURRENT TELEPHONY ENVIRONMENT*

The West Virginia Department of Administration's current IP telephony environment as it applies to this RFP is comprised of a combination of State administered Cisco Unified Communications Manager (CUCM), and hosted and managed Unified Communication and Collaboration as a Service (UCCaaS) deployments serving approximately 10,000 employees throughout the State. The State is actively working to transition to the hosted UCCaaS service and the information provided below represents a "snapshot in time" as of this writing. All figures stated are estimates only and are subject to change.

The State's Wide Area Network is comprised of over 500 sites that are connected to the network core in Charleston, West Virginia. Of these, approximately 425 agency locations are connected via Verizon provided MPLS, approximately 50 utilize DSL, and the remaining balance is made up of Cable (Internet VPN), Point-to-Point, and T1 Circuits.

## *SECTION 1: CISCO UNIFIED COMMUNICATIONS*

The Department of Administration has multiple Cisco Unified Communications Manager (CUCM) deployments (Versions 4.x, 7.x, & 10.x) supporting approximately 9,000 stations. Additionally, there are nineteen (19) Unified Communications Manager Express / Unity Express (CME/CUE) installations supporting approximately 800 additional stations. These systems utilize a combination of SIP, PRI, and Centrex/POTS circuits for in-bound and out-bound dialing. The diagram and tables below provide an overview of the State's existing IPT infrastructure.

## *DIAGRAM 1.1: CALL MANAGER ENVIRONMENT – LOGICAL VIEW*

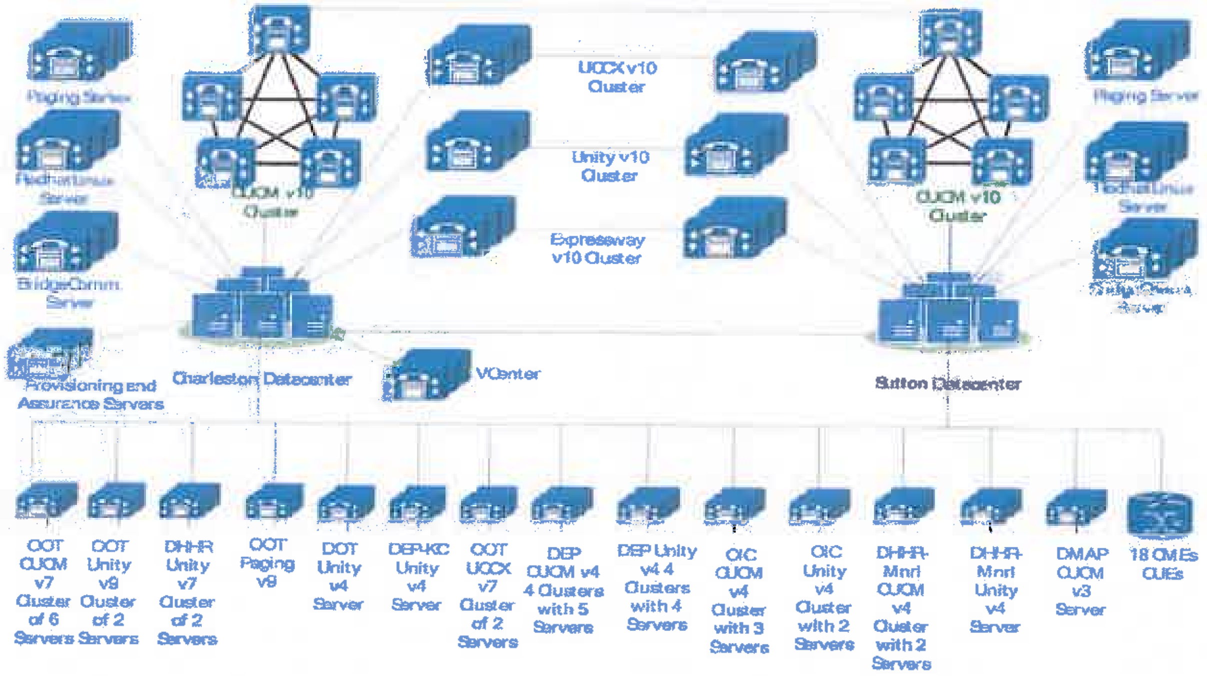

Paging Server
RedHat Linux Server
BridgeComm Server
Provisioning and Assurance Servers
CUCM v10 Cluster
Charleston Datacenter
UCCX v10 Cluster
Unity v10 Cluster
Expressway v10 Cluster
VCenter
CUCM v10 Cluster
Sutton Datacenter
Paging Server
RedHat Linux Server
BridgeComm Server
OOT CUCM v7 Cluster of 6 Servers
OOT Unity v9 Cluster of 2 Servers
DHHR Unity v7 Cluster of 2 Servers
OOT Paging v9
DOT Unity v4 Server
DEP-KC Unity v4 Server
OOT UCCX v7 Cluster of 2 Servers
DEP CUCM v4 4 Clusters with 5 Servers
DEP Unity v4 4 Clusters with 4 Servers
OIC CUCM v4 Cluster with 3 Servers
OIC Unity v4 Cluster with 2 Servers
DHHR-Mnrl CUCM v4 Cluster with 2 Servers
DHHR-Mnrl Unity v4 Server
DMAP CUCM v3 Server
18 CMEs CUEs

***TABLE 1.1: CISCO CALL MANAGER CLUSTERS:***

| Cluster | Number of Supported Sites | Estimated Number of Phones |
|---|---|---|
| CCM4 | 8 | 1,038 |
| CUCM7 | 165 | 7,848 |
| CUCM10 | 22 | 1,306 |
| CME/CUE | 19 | 800 |

***TABLE 1.2: LISTING OF STATE LOCATIONS CURRENTLY UTILIZING IPT:***

| Address | City | State | Zip |
|---|---|---|---|
| 50 Rocky Branch Road | Alum Creek | WV | 25003 |
| 105 S. Eisenhower Drive | Beckley | WV | 25801 |
| 109 East Main Street | Beckley | WV | 25801 |
| 800 New River Town Center | Beckley | WV | 25801 |
| 101 Cambridge Place | Bridgeport | WV | 26330 |
| 83 Brushy Fork Road | Buckhannon | WV | 26201 |
| 2120 N Western Turnpike | Burlington | WV | 26710 |
| 1007 Bullitt Street Suite 400 | Charleston | WV | 25301 |
| 101 Dee Drive Suite 103 | Charleston | WV | 25311 |
| 107 Capitol Street | Charleston | WV | 25301 |
| 1124 Smith Street | Charleston | WV | 25301 |
| 1201 Greenbrier Street | Charleston | WV | 25311 |
| 1207 Quarrier Street | Charleston | WV | 25301 |
| 1321 Plaza East | Charleston | WV | 25303 |
| 1340 Smith Street | Charleston | WV | 25301 |
| 1356 Hansford Street | Charleston | WV | 25301 |
| 1409 Greenbrier Street | Charleston | WV | 25311 |
| 1409 Washington Street | Charleston | WV | 25301 |
| 1596 Kanawha Blvd. E | Charleston | WV | 25311 |
| 190 Dry Branch Drive | Charleston | WV | 25306 |
| 1900 Kanawha Blvd | Charleston | WV | 25305 |
| 2019 Washington Street E | Charleston | WV | 25305 |
| 208 Hale Street | Charleston | WV | 25301 |
| 2101 Washington Street E | Charleston | WV | 25305 |
| 231 Capitol Street | Charleston | WV | 25301 |
| 300 Capitol Street | Charleston | WV | 25301 |
| 350 Capitol Street | Charleston | WV | 25301 |
| 4101 MacCorkle Ave SE | Charleston | WV | 25304 |
| 4190 Washington Street W | Charleston | WV | 25313 |
| 4701 MacCorkle Ave SE | Charleston | WV | 25304 |
| 4752 Chimney Drive | Charleston | WV | 25302 |

| | | | |
|---|---|---|---|
| 502 Eagle Mountain Road | Charleston | WV | 25311 |
| 505 Capitol Street Suite 200 | Charleston | WV | 25301 |
| 515 Central Ave | Charleston | WV | 25302 |
| 5707 MacCorkle Ave SE | Charleston | WV | 25317 |
| 601 57th Street SE | Charleston | WV | 25304 |
| 617 Leon Sullivan Way | Charleston | WV | 25301 |
| 619 Virginia Street W | Charleston | WV | 25302 |
| 7 Players Club Drive Suite 2 | Charleston | WV | 25311 |
| 723 Kanawha Blvd E. Suite 700 | Charleston | WV | 25301 |
| 816 Quarrier Street Suite 300 | Charleston | WV | 25301 |
| 900 Pennsylvania Ave | Charleston | WV | 25302 |
| One Davis Square | Charleston | WV | 25301 |
| One Players Club Drive | Charleston | WV | 25311 |
| Robert C. Byrd United States Courthouse | Charleston | WV | 25301 |
| 908 Bullitt Street | Charleston | WV | 25301 |
| National Guard Armory | Charleston | WV | 25311 |
| 153 West Main Street Suite B | Clarksburg | WV | 26301 |
| 2460 Murphy's Run Road | Clarksburg | WV | 26301 |
| 284 Factory Street Suite 102 | Clarksburg | WV | 26301 |
| 137 Peach Court Suite 2 | Danville | WV | 25053 |
| 141 Forestry Camp Road | Davis | WV | 26260 |
| 1201 Dunbar Ave | Dunbar | WV | 25064 |
| 1023 N. Randolph Ave | Elkins | WV | 26241 |
| 1025 N. Randolph Ave | Elkins | WV | 26241 |
| 494 Elkview River Road S | Elkview | WV | 25071 |
| 2031 Pleasants Valley Road Suite 1 | Fairmont | WV | 26554 |
| 320 Adams Street | Fairmont | WV | 26554 |
| 416 Adams Street | Fairmont | WV | 26544 |
| 420 Marion Square | Fairmont | WV | 26554 |
| 1159 Nick Rahall Greenway | Fayetteville | WV | 25840 |
| 156 Resource Lane | Foster | WV | 25081 |
| 409 Wood Mountain Road | Glen Jean | WV | 25880 |
| 103 Academy Street | Glenville | WV | 26351 |
| 85 Industrial Park Road | Grantsville | WV | 16147 |
| 801 Madison Ave | Huntington | WV | 25701 |
| 115 Liberty Square | Hurricane | WV | 25526 |
| 24 Ruland Road | Kearneysville | WV | 25430 |
| 18 N. Tornado Way | Keyser | WV | 26726 |
| 67 N. Tornado Way | Keyser | WV | 26726 |
| 146 Stonehouse Road | Lewisburg | WV | 24901 |
| 3293 Jefferson Street N. Suite 105 | Lewisburg | WV | 24901 |
| 1101 George Kostas Drive | Logan | WV | 25601 |
| 130 Stratton Street | Logan | WV | 25601 |

| | | | |
|---|---|---|---|
| 467 Main Street Suite 401 | Madison | WV | 25130 |
| 1014 South Raleigh Street | Martinsburg | WV | 25401 |
| 200 Viking Way | Martinsburg | WV | 25402 |
| 38 Severna Parkway | Martinsburg | WV | 25404 |
| 433 Mid-Atlantic Park | Martinsburg | WV | 25402 |
| 120 Water Plant Drive | Moorefield | WV | 26836 |
| 149 Robert C. Byrd Industrial Park | Moorefield | WV | 26836 |
| 114 High Street | Morgantown | WV | 26507 |
| 1415 Earl Core Road | Morgantown | WV | 26505 |
| 1525 Decker's Creek Blvd | Morgantown | WV | 26505 |
| 304 Scott Ave | Morgantown | WV | 26508 |
| 5000 Greenbag Road | Morgantown | WV | 26501 |
| 901 8th Street | Moundsville | WV | 26041 |
| 10 McJunkin Road | Nitro | WV | 25143 |
| 550 Industrial Drive | Oak Hill | WV | 25901 |
| 549 Mall Road | Oak Hill | WV | 25901 |
| 225 Holiday Hills Drive | Parkersburg | WV | 26101 |
| 300 Lakeview Center | Parkersburg | WV | 26101 |
| 400 5th Street | Parkersburg | WV | 26101 |
| 601 Lubeck Ave | Parkersburg | WV | 26101 |
| 907 Mission Drive | Parkersburg | WV | 26101 |
| 9346 Seneca Trail | Parsons | WV | 26287 |
| 53 Kiess Drive | Petersburg | WV | 26847 |
| 47 School Street Suite 301 | Philippi | WV | 26416 |
| 1767 Bearhole Road | Pineville | WV | 24874 |
| 1406 Kanawha Street | Point Pleasant | WV | 25550 |
| 2807 Jackson Ave. Suite 200 | Point Pleasant | WV | 25550 |
| 1 Walden Roush Way | Point Pleasant | WV | 25550 |
| 270 Hardwood Lane | Princeton | WV | 24740 |
| 901 Shelter Road | Princeton | WV | 24740 |
| 1186 North Mildred Street | Ranson | WV | 25438 |
| 24948 Northwestern Pike | Romney | WV | 26757 |
| 22278 Northwestern Pike | Romney | WV | 26757 |
| 22 Herbert Ave | Smithburg | WV | 26436 |
| 324 4th Ave | South Charleston | WV | 25303 |
| 115 Church Street | Spencer | WV | 25276 |
| 321 Market Street | Spencer | WV | 25276 |
| 570 West MacCorkle Ave | St. Albans | WV | 25177 |
| 808 B Street Suite G | St. Albans | WV | 25177 |
| 1655 S. Pleasants Highway | St. Marys | WV | 26170 |
| 707 Professional Park Drive | Summersville | WV | 26651 |
| 89 Richard Minnich Drive | Sutton | WV | 26601 |
| 3708 Sutton Lane | Sutton | WV | 26601 |

| | | | |
|---|---|---|---|
| Putnam Village Shopping Center | Teays | WV | 25569 |
| 1400 12th Street | Vienna | WV | 26105 |
| 100 Municipal Plaza | Weirton | WV | 26062 |
| 110 Park Ave. Suite 100 | Welch | WV | 24801 |
| 830 Virginia Ave | Welch | WV | 24801 |
| 840 Virginia Ave | Welch | WV | 24801 |
| 225 Depot Street | Weston | WV | 26452 |
| 306 Market Place Mall | Weston | WV | 26452 |
| 11 Commerce Drive Suite 204 | Westover | WV | 26501 |
| 14 Commerce Drive Suite 1 | Westover | WV | 26501 |
| 1324 Chapline Street Suite 200 | Wheeling | WV | 26003 |
| 69 16th Street | Wheeling | WV | 26003 |
| 225 E 3rd Ave | Williamson | WV | 25661 |
| 12531 Winfield Road | Winfield | WV | 25213 |
| 3266 Winfield Road | Winfield | WV | 25213 |

***TABLE 1.3: INSTALLED CISCO PHONE MODELS:***

The State has made a large investment in Cisco phone sets and requests that the Vendor allow the State to continue to use these sets until they are no longer supported by Cisco or the Operating System Software. At which time, the Vendor will replace the set.

| Phone Model | Quantity |
|---|---|
| Cisco 6921 | 36 |
| Cisco 7905 | 10 |
| Cisco 7906 | 1 |
| Cisco 7911 | 1 |
| Cisco 7921 | 7 |
| Cisco 7925 | 10 |
| Cisco 7931 | 1453 |
| Cisco 7936 | 35 |
| Cisco 7937 | 103 |
| Cisco 7940 | 802 |
| Cisco 7941 | 781 |
| Cisco 7942 | 2090 |
| Cisco 7945 | 537 |
| Cisco 7960 | 815 |
| Cisco 7961 | 703 |
| Cisco 7962 | 434 |
| Cisco 7965 | 95 |
| Cisco 7970 | 8 |
| Cisco 7975 | 34 |
| Cisco 8811 | 774 |

| | |
|---|---|
| Cisco 8831 | 38 |
| Cisco 8851 | 40 |
| Cisco 8861 | 3 |
| Cisco 8941 | 508 |
| Cisco 8945 | 1 |
| Cisco 8961 | 13 |
| Cisco 9951 | 3 |
| Cisco ATA 186 | 12 |
| Cisco ATA 187 | 2 |
| Cisco IP Communicator | 36 |
| Cisco Unified Client Services Framework | 10 |
| Third-party AS-SIP Endpoint | 3 |
| Third-party SIP Device (Advanced) | 1 |
| Total | 9399 |

## *SECTION 2: HOSTED UCCaaS (VERIZON BUSINESS)*

The State has an active contract with Verizon Business to provide a hosted and managed Unified Communications and Collaboration as a Service (UCCaaS) cloud-based service. The State expects the winning Vendor to transition all sites utilizing this service to their hosted solution prior to the expiration of the contract in October 2019. Table 2.1 below lists the agencies that are currently utilizing this service.

### *TABLE 2.1: STATE AGENCIES ON HOSTED UCCaaS:*

| Agency | Number of Supported Sites | Estimated # of Phones |
|---|---|---|
| Tax and Revenue | 5 | 440 |
| Department of Juvenile Services | 1 | 33 |
| Governor's Office and Mansion | 2 | 82 |
| Office of Tax Appeals | 1 | 10 |

## *SECTION 3: CISCO UNIFIED CONTACT CENTER EXPRESS*

The State's Cisco Unified Contact Center Express deployment is hosted on the CUCM 7.x system and supports eight (8) state call centers serving and estimated 500 contact center agents. The State expects the winning Vendor to transition the Call Centers to the Vendor's hosted virtual environment. Table 3.1 below lists the Call Centers that are currently supported on the State's CUCM 7.x system.

### *TABLE 3.1: CUCM 7.x CALL CENTERS:*

| Agency / Contact Center | Estimated # of Agents |
|---|---|
| Public Employees Insurance Agency | 73 |
| Administration-Office of Technology Service Desk | 50 |

| | |
|---|---|
| Bureau of Children and Families (DHHR) | 75 |
| Bureau for Child Support Enforcement (DHHR) | 23 |
| DHHR-Poison Control Center | 30 |
| Department of Transportation (DOT/DMV) | 220 |
| Department of Commerce | 20 |
| WV Business Line | 1 |

## ***SECTION 4: VIRTUAL CONTACT CENTER (VERIZON BUSINESS)***

The State is currently utilizing Verizon's Virtual Contact Center service at two state agencies serving approximately 85 agents. The State expects the virtual contact centers listed below in Table 4.1 to be converted to the Vendor's hosted virtual solution as part of this contact.

### ***TABLE 4.1: VIRTUAL CONTACT CENTERS:***

| Agency / Call Center | Estimated # of Phones |
|---|---|
| Department of Health and Human Resources (Central Intake Center) | 43 |
| Department of Health and Human Resources (Charleston Call Center) | 56 |
| Department of Tax and Revenue Services | 20 |

## ***SECTION 5: 24 HOUR STATE FACILITIES***

The State facilities listed in Table 5.1 below require 24x7x365 support. No additional charges or overtime will be authorized or paid if work is performed outside of Vendor's standard business hours.

### ***TABLE 5.1: 24 HOUR FACILITIES***

| Site | Location | City | State | Zip |
|---|---|---|---|---|
| Jackie Withrow Hospital | 105 S. Eisenhower Drive | Beckley | WV | 25801 |
| BCF – Centralized Intake | 350 Capitol Street | Charleston | WV | 25301 |
| OEMS - NOROP | 89 Richard Minnich Drive | Sutton | WV | 26601 |
| DJS - Lorrie Yeager Jr Juvenile Services | 907 Mission Drive | Parkersburg | WV | 26101 |
| DJS – Rubenstein Juvenile Center | 141 Forestry Camp Road | Davis | WV | 26260 |
| DOC – Parkersburg Correctional Center | 225 Holiday Hills Drive | Parkersburg | WV | 26104 |
| DHHR- Center for Threat Preparedness | 505 Capitol St. Suite 200 | Charleston | WV | 25301 |
| DHHR- Chief Medical Examiner | 619 Virginia St W | Charleston | WV | 25302 |
| DMAPS - Homeland Fusion Center | 1900 Kanawha Blvd. | Charleston | WV | 25305 |
| DOC - Charleston Correctional Center | 1356 Hansford Street | Charleston | WV | 25301 |
| DOT- Traffic Management Center | 1900 Kanawha Blvd., E. | Charleston | WV | 25305 |

| | | | | |
|---|---|---|---|---|
| DHSEM - Homeland Security and Emergency Management | National Guard Armory, 1703 Coonskin Drive | Charleston | WV | 25311 |

# Appendix B. Addendum Acknowledgement(s)

Please reference the Addendum Acknowledgement(s) provided on the following page(s).

## ADDENDUM ACKNOWLEDGEMENT FORM
## SOLICITATION NO.: CRFP 0212 SWC1900000001

**Instructions:** Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

**Acknowledgment:** I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

**Addendum Numbers Received:**
(Check the box next to each addendum received)

☑ Addendum No. 1
☑ Addendum No. 2
☑ Addendum No. 3
□ Addendum No. 4
□ Addendum No. 5
□ Addendum No. 6
□ Addendum No. 7
□ Addendum No. 8
□ Addendum No. 9
□ Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Verizon Business Network Services Inc. on behalf of MCI Communications Services, Inc. dba Verizon Business Services
Company

Authorized Signature

November 20, 2018
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

# ADDENDUM ACKNOWLEDGEMENT FORM
## SOLICITATION NO.: CRFP 0212 SWC1900000001

**Instructions:** Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

**Acknowledgment:** I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

**Addendum Numbers Received:**
(Check the box next to each addendum received)

☑ Addendum No. 1
☑ Addendum No. 2
☑ Addendum No. 3
☑ Addendum No. 4
□ Addendum No. 5
□ Addendum No. 6
□ Addendum No. 7
□ Addendum No. 8
□ Addendum No. 9
□ Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Verizon Business Network Services Inc. on behalf of MCI Communications Services, Inc. dba Verizon Business Services
Company

Authorized Signature

November 20, 2018
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

# ADDENDUM ACKNOWLEDGEMENT FORM
## SOLICITATION NO.: CRFP 0212 SWC1900000001

**Instructions:** Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

**Acknowledgment:** I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

**Addendum Numbers Received:**
(Check the box next to each addendum received)

☑ Addendum No. 1<br>
☑ Addendum No. 2<br>
☑ Addendum No. 3<br>
☑ Addendum No. 4<br>
☑ Addendum No. 5

□ Addendum No. 6<br>
□ Addendum No. 7<br>
□ Addendum No. 8<br>
□ Addendum No. 9<br>
□ Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Verizon Business Network Services Inc. on behalf of MCI Communications Services, Inc. dba Verizon Business Services

Company

Authorized Signature

November 20, 2018

Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

# Appendix C. Verizon VCC Powered by NICE inContact Security

Please refer to our attached icon(s) below, pertaining to the Verizon Virtual Contact Center (VCC) Powered by NICE inContact Security documentation. For hardcopy purposes, please review the following page(s).

inContact Security Statement.pdf

NICE inContact Security Program.pdf

NICE inContact Technical FAQ.PDF

# inContact Security Statement

## Introduction

Businesses today leverage cloud services to solve and address their business needs because these services are cost effective, elastic, scalable, and configurable. While benefits are demonstrable and significant, surveys indicate that one of the primary concerns for customers considering cloud services is security.

inContact maintains a layered approach that presents a profile of inContact defense-in-depth to assure customers/tenants that their data is managed securely. This document addresses those measures that inContact maintains to safeguard a customer's data security layers.

## inContact Cloud Service Security Objectives

In order to implement and properly maintain a robust information security function, inContact, overseen by the Trust Office, recognizes the importance of and takes steps to ensure:

- Understanding inContact's information security requirements and the need to establish policy and objectives for information security
- Implementing operating controls to manage inContact information security risks in the context of overall business risks
- Ensuring all users of inContact information assets are aware of their responsibilities in protecting those assets
- Monitoring and reviewing the performance and effectiveness of information security policies and controls
- Continual improvement based on assessment, measurement and changes that affect risk
- Initiating action to define, detect, assign, and assure that threats are managed
- Maintain a structure that allows discrete employee assignments for the policies, procedures and practices necessary for security, along with training and tools to maintain varied security features.

**This document reflects inContact's current processes and procedures, which may change from time to time as best practices and business needs evolve. This document is for informational purposes only. inContact MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. Nothing in this document shall create any legal obligations or rights.**

# Data Center and Physical Security

inContact operates in geographically diverse, carrier grade data centers. Each data center is equipped with security measures designed for a high level of security and reliability. These measures include:

- Geographically diverse data centers, with locations in Dallas TX and Los Angeles CA.
    - Level 3 providing the data center in Dallas and Coresite in Los Angeles
- Emergency, building supplied generators and UPS for back-up power
- Dual-interlock, pre-action, dry-pipe fire suppression
- Earthquake and explosion resistant construction
- Environmental climate controls – fully redundant cooling
- Raised flooring and floor to true ceiling walls
- 24x7 closed-circuit video
- Card access
- Alarmed doors
- Redundant and multiple transmission services facility entrances

# System Account Controls

inContact utilizes measures to control unauthorized access to its network and systems. These measures include:

- Unique identifiers for system access
- Logging and monitoring of system acess
- Multi-factor authentication for all remote access to production systems

**This document reflects inContact's current processes and procedures, which may change from time to time as best practices and business needs evolve. This document is for informational purposes only. inContact MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. Nothing in this document shall create any legal obligations or rights.**

# Data Storage Security

Secure delivery, and protection of customer data are key components of inContact services. inContact employs the following data security measures:

- Role-based access controls
- Raid 10 3PAR encrypted storage arrays (SAN)
- Data backups and site to site real time data replication
- Encrypted FTP storage solutions
- Data destruction procedures end of life systems

# Data Transmission and Network Security

inContact ensures the confidentiality and integrity of customer data in transit

- Secure data transmission using HTTPS port 443
- Next generation firewalls with IDS/IPS
- VPN services available for certain services including VoIP
- Secure MPLS services for VoIP
- Separate Production and Administration networks
- Monthly network scans (Qualys)
- Internal vulnerability scanning (Nessus)
- Yearly penetration testing by a 3rd party
- Web services hosted from secure DMZ's
- SFTP data transfer services

# Separation of Data

inContact implements measures that ensure the separate processing of data collected for different purposes.
The separation of data processing is accomplished by:

- Access to data between tenants or business units is separated through application security to restrict access appropriately by user profile
- Information in database uses unique business unit identifiers to logically separate tenant data
- Administrative access to data is restricted to small number of closely managed inContact administrators
- Access to data in the databases is done through stored procedures using only approved accounts
- Access to the database is only allowed from trusted servers

**This document reflects inContact's current processes and procedures, which may change from time to time as best practices and business needs evolve. This document is for informational purposes only. inContact MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. Nothing in this document shall create any legal obligations or rights.**

## Management

Eyes on the network, monitoring performance and security is integral to inContact's Security Program

- 7 x 24 Global Network Operations Center (NOC)
  - Salt Lake City and Philippines
- Alerting tools to notify NOC about system performance
- Security logging and alerting
- Formalized change management process
- Anti-virus protection
- Monthly patch management
- Segregation of duties between development, deployment and operations
- Change validation procedures

## Compliance

inContact management of information and information assets are subject to statutory, regulatory, and contractual security requirements. inContact maintains an Internal Audit department with dedicated officers to comply with state, federal and international requirements.

- PCI
- SOX 404 (Mandated by SEC with annual report found on SEC.GOV)
- Customer Proprietary Network Information (CPNI)
- U.S. and international export controls
- PUC & FCC telecom regulations
- CVAA Communication and Video Accessibility Act
- European Union privacy requirements
- Safe Harbor
- SOC 2 Type 2
- Red Flag Rule – Identity Theft

**This document reflects inContact's current processes and procedures, which may change from time to time as best practices and business needs evolve. This document is for informational purposes only. inContact MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. Nothing in this document shall create any legal obligations or rights.**

## Secure Development

The core level of security controls at inContact is centered on secure development of our software platform. inContact employs development measures including:

- Agile development (SCRUM)
- .Net managed code to enhance security
- Source code management using Microsoft Team Foundation Server
- Secure code training
- Application of OWASP principles for coding and QA
- Multiple environments: development, test, staging, beta and production
- Regression testing
- Redundant and fault tolerant application design

NICE · inContact

# Security Program
# Trust Office

**V 3.4**

**September 2017**

## Table of Contents

# Section 1: Introduction

## Definitions

**Cloud:** Computing, storage, telecom and software services, using an IaaS, PaaS or SaaS infrastructure delivery model, that are hosted and managed in all or part by an external provider, that provides elastic capacities and access to services via a web or VPN interface.

**Control:** Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature.

**Information Asset:** Non-tangible item that has value to the company.

**Information Security:** Preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

**Physical Asset:** Tangible item that has value to the company.

**Policy:** Overall intention and direction as formally expressed by management.

**Risk:** The likelihood of a threat agent taking advantage of vulnerability and the resulting business impact.

**Risk Assessment:** Overall process of risk analysis and risk evaluation.

**Risk Evaluation:** Process of comparing the estimated risk against given risk criteria to determine the significance of the risk.

**Risk Management:** Coordinated activities to direct and control the agency with regard to risk.

**Threat:** A potential cause of an unwanted incident, which may result in harm to a system or the agency.

**Vulnerability:** A weakness of an asset or group of assets that can be exploited by one or more threats.

## Authority (Policy & Procedure list)

| Policies* | Start Date |
|---|---|
| Change Management Policy | 11-26-2008 |
| Anti-Fraud Policy | 10-08-2007 |
| Contracting Policy | 05-11-2010 |
| Mobile Device Policy and Procedure | 02-01-2011 |

| | |
|---|---|
| Mobile Device Acceptable Use Policy | 11-13-2012 |
| Red Flags Policy | 12-02-2010 |
| Employee Handbook | 02-01-2011 |
| NICE Code of Ethics | 06-07-2007 |
| Computer Network Security Policy | 12-02-2010 |
| Document Retention Policy | 07-08-2009 |
| Fixed and Intangible Asset Policy | 11-17-2009 |
| Standard Operating Procedure Policy | 11-11-2010 |
| Personnel Security Policy | 10-26-2012 |
| Remote Telecommuting Policy | 04-3-2013 |
| Encryption Security Policy | 10-26-2012 |
| System Maintenance Policy | 10-26-2012 |
| Server Security Policy | 07-05-2012 |

| Procedures* | Start Date |
|---|---|
| Help Desk Process Manual | 09-27-2010 |
| Bill Cycle Processing | 11-11-2010 |
| Critical Vendor Process | 11/20/2012 |
| Customer Setup and Contract Review | 10-22-2010 |
| Alarms and Alerts Response | 10-27-2010 |
| Incident Management Plan | 11-19-2014 |
| Incident Management Process | 05-18-2010 |
| Employee Termination Procedures | 01-01-2011 |
| Log File Process | 01-01-2012 |
| New Employee Background Check | 10-10-2010 |
| New Employee Drug Screen | 10-28-2010 |
| Security Access Badge Process | 10-28-2010 |
| Data Center Maintenance/Work Guide Lines | 12-15-2009 |
| NICE inContact Technical Controls | 09-30-2010 |
| Network Architecture Confidentiality | 10-23-2013 |
| Whistleblower Response Process | 05-18-2010 |
| New Hire Process | 09-26-2012 |
| Technical Support & NOC Disaster Recovery | 05-23-2013 |
| System Configuration Document Process | 11-1-2013 |
| Secure Development Lifecycle | 09-12-2014 |

| Certifications/Reports* | Start Date |
|---|---|
| PCI | 12-31-2010 |
| CPNI | 01-01-2010 |
| FedRAMP Assess Only (Federal Risk and Authorization Management Program approval from Army Medical) | 07/31/2017 |
| SOX 404 | 12-31-2010 |
| SOC 2 Type II (SAS70) | 12-31-2010 |
| Safe Harbor | 04-21-2009 |
| ICO Data Protection Registration | 11-19-2010 |

* The above policies, procedures, and Certifications are reviewed/renewed annually.

## Roles and Responsibilities

**CSO**

Responsible for information security in the company, for reducing risk exposure, and for ensuring the company's activities do not introduce undue risk. The Chief Security Officer also oversees and directs compliance with government and regulatory standards, security initiatives, and security policies.

**Trust Office Director**

Responsible for ensuring compliance with existing security policies, analyzing effectiveness of existing security policies, and developing and training new security policies and procedures.

**Corporate Compliance and Internal Audit Director**

Responsible for company compliance with current and future compliance, internal regulatory and government requirements and reporting. The Director of Corporate Compliance and Internal Audit are also responsible for communicating with the Risk Assessment Committee and reporting security incidents.

**Compliance Department**

Responsible for the coordination and completion of all government, regulatory, and compliance documents for all entities nationally and internationally.

**Information Owner**

Responsible for creating initial information classifications, approving decisions regarding controls and access privileges, and ensuring regular reviews to manage changes to risk.

**User**

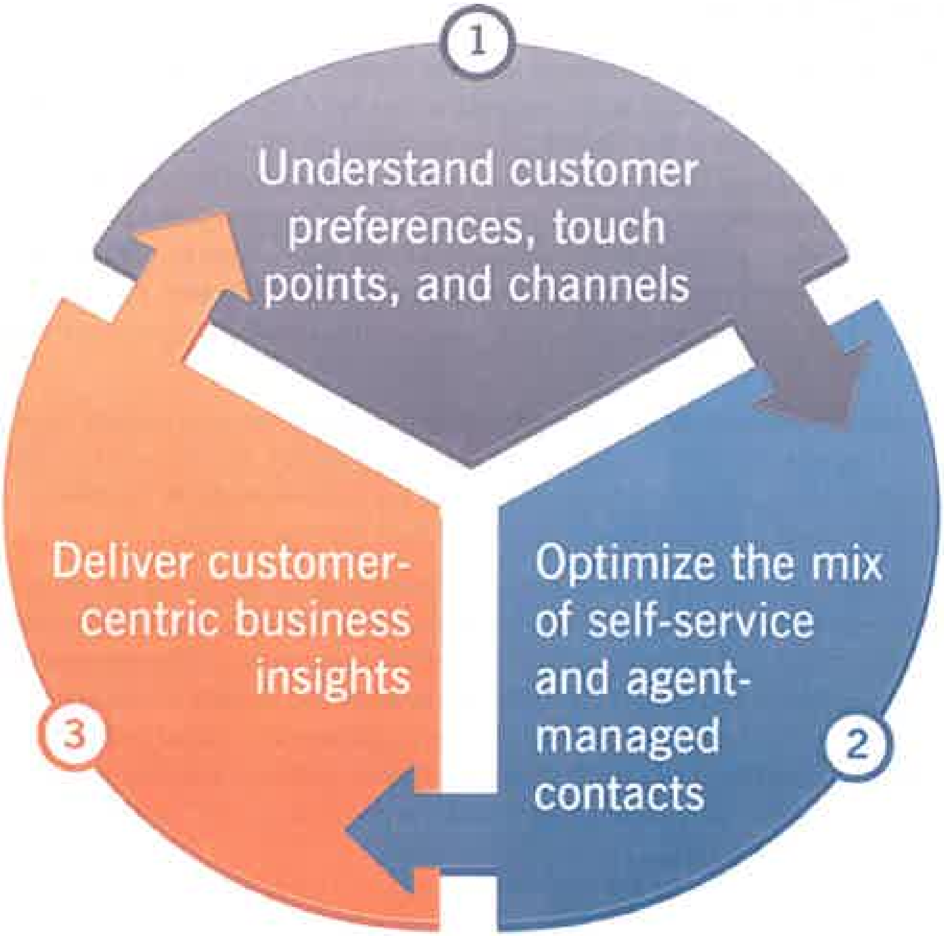
Responsible for complying with policies, procedures, and practices.

# About NICE inContact

NICE inContact, Inc. has been purchased by NICE Systems of Paramus, New Jersey. NICE inContact continues to function as a corporate entity. NICE inContact and subsidiaries employ over 1200 people in the United States and abroad. NICE inContact helps call centers around the globe create profitable customer experiences through its powerful portfolio of cloud-based call center call routing, self-service and agent optimization solutions. The company's services and solutions enable call centers to operate more efficiently, optimize the cost and quality of every customer interaction, create new pathways to profit and ensure ongoing customer–centric business improvement and growth.

NICE inContact technical infrastructure allows for multiple choices of carriers to prevent disaster and individual carrier outages from impacting service. Its active-active database and redundant device architecture assures highly available services. Its flexible data stores allow for elastic capacity management of data storage capacity.

NICE inContact's sophisticated cloud-based technology gives customer call centers many advantages not available with traditional premise-based systems. Aside from being far more cost effective, NICE inContact allows call centers to create a differentiated and profitable customer experience. NICE inContact enables call centers to understand their customer preferences, touch points, and channels; optimize the mix of self-service and agent-managed contacts; and deliver customer-centric business insights. To learn more about NICE inContact, visit www.incontact.com. For more about the parent company NICE Ltd., visit www.nice.com.


1
Understand customer preferences, touch points, and channels
2
Optimize the mix of self-service and agent-managed contacts
3
Deliver customer-centric business insights

The NICE inContact platform includes an ACD with skills-based routing, IVR with speech recognition, CTI capabilities, reporting, Workforce Optimization, Dialer, API (customer's and/or developers use API to develop solutions), and hiring and customer feedback measurement tools. Together, the NICE inContact platform creates an integrated, all-in-one solution for operations seeking to support call centers, including those with a distributed workforce, either at-home or multi-site. **

** Ventana Research

# Section 2: Security Governance

## Security Program Objective

Many businesses today are interested in using Cloud services to solve and address their business needs. Cloud services are of interest for these businesses because such services are cost effective, elastic, scalable, and configurable. While these benefits are significant, many customers are concerned that using a Cloud provider will negatively impact their ability to operate securely.

Information and operational security are critical business issues for both NICE inContact and its customers. The objective of security is to identify risks, assess, and take steps to avoid or mitigate those risks to the information assets of NICE inContact and its customers.

In order to implement and properly maintain a robust information security function, NICE inContact, overseen by the Trust Office, recognizes the importance of and takes steps to insure:

- Understanding NICE inContact's information security requirements and the need to establish policy and objectives for information security
- Implementing and operating controls to manage NICE inContact information security risks in the context of overall business risks
- Ensuring all users of NICE inContact information assets are aware of their responsibilities in protecting those assets
- Monitoring and reviewing the performance and effectiveness of information security policies and controls
- Continual improvement based on assessment, measurement and changes that affect risk
- Initiating action to define, detect, assign, and assure that threats are managed
- Discrete employee assignments, along with training and tools to maintain
    - Vulnerability and penetration assessments (Trust Office scan and pen testing processes, procedures, and action plans);
    - Security assessment measures within the network (NOC department monitoring and alerting backed by processes and tools), Network Architecture, Network Engineering, and Systems Administration departments as SMEs to go along with monitored device process (Edge devices, IDS, IPS, etc.); Scanning traffic and configurations (BMC Truesite) and Training (department specific security training).
    - Security documentation. (Specific members of the Trust Office manage and deliver artifacts and security assurance to internal and external requestors. And the Internal Audit department verifies content of such artifacts as this NICE inContact Security Program, a SOC 2 Type 2 Report, a PCI Attestation of Compliance, a Privacy Policy, and the many policies a standard operating procedure document that define specific vertical responsibilities. The Trust Office assures that these security documents are complied with inside the organization.)
    - Disaster recovery/business continuity plans. (The Trust Office assigns a person to be responsible for reviewing and updating the Resiliency Event Management plan with an executive summary.)

- Compliance with various security verification infrastructures. (An Internal Audit/Trust Department which schedules and executes audits. These audits produce such artifacts as SOC 2 Type 2 Report, PCI Attestation of Compliance, Privacy Policy including Privacy Shield, HITRUST and assure adherence to the many policies and standard operating procedure documents that define specific vertical responsibilities that relate to internal and customer security. These artifacts are reviewed on a regular basis.)
- Compliance with policies and procedures. (An assigned member of the Internal Audit Department is a compliance subject matter expert, and evaluates, creates, and schedules Security Awareness, Policy, European Data Directive and the upcoming GRDP, and HIPAA Training which is delivered to all or appropriate members of NICE inContact's workforce.)
- Detection and prevention of system failures. (NOC subject matter experts are tasked with monitoring and alerting systems, and are backed by processes and tools), monitored device process (Edge devices, IDS, IPS, etc.); Scanning traffic and configurations (BMC Truesight) Training (group specific security training.)

# Security Components

## *Governance*

Governance is an essential component for the long-term strategy and direction of NICE inContact with respect to the security policies and risk management program. Governance requires executive management involvement, approval, and ongoing support. It also requires an organizational structure that can inform and advise executive, business and information technology management on security issues and acceptable risk levels.

### Governance Structure

**The Executive Committee** is comprised of the executive officers of NICE inContact and is responsible for the strategy and day to day operations which include the oversight of the security programs and policies.

**The Steering Committee** is comprised of the executive officers of NICE inContact. The Steering Committee is responsible for all NICE inContact policies as well as the prioritizing and mitigation of risks.

**The Risk Assessment Committee** is comprised of individuals from within the Company. The committee identifies and evaluates risks that exist from an operational and financial perspective. This committee considers and recommends formal processes and procedures to assess and mitigate risk in these various areas. Ultimately this committee is responsible to identify and ensure mitigation of identified risk. If risks are not mitigated the committee is responsible for ensuring that management is not only aware of but has accepted said risk factors.

**Internal Audit** consists of trained auditors and compliance personnel. This team provides assurance through audits, develops and reviews internal policies and procedures, coordinates and manages external auditors and audit processes, and performs necessary regulatory, compliance and incident reporting. This team is independent from the Company which ensures compliance with regulations and company policies and procedures by performing audit procedures. It is responsible for Enterprise Risk Management, identifying and recommending to management course of action that would eliminate or reduce identified risk factors. Internal Audit consults with management on all strategic areas including security.

The Trust Office is tasked with leveraging best industry security practices into NICE inContact transparency. Transparency gives assurances to both customers and auditors that NICE inContact protects customer data. The Trust Office's mandate is to apply to the NICE inContact's business the principles of high reliability, high performance, and high security.

**The Trust Office** consists of Company employees trained in security methods. This team works within the Company to identify risks and develop methods to mitigate those risks. This team creates training, coordinates and supports operational security activities for business continuity planning, disaster recovery, best practices, standard operating procedures, product security and testing.

An important part of Trust's charter is identification and remediation of risks from security threats. Trust performs regular scans and testing (see *Testing NICE inContact Vulnerability Surfaces* heading in Compliance section below) of its Cloud threat surfaces using qualified resources and tools.

**Human Resources** (HR) consists of Company employees trained in the administration of personnel. HR is responsible for administration of company employee policies and procedures as well as hiring and termination policies and procedures.

**Training** is comprised of Company employees. Training is responsible for training customers on NICE inContact products and services, and provides training to employees on Company tools, methods, procedures and policies, including security awareness training and the company policy handbook.

**NICE inContact Managers** are responsible for the administration of their respective teams and the implementation of Company policies and procedures.

## *Risk Management*

Risk Management is about identifying potential threats -- the probability, likelihood and impact of threats to the company. Economy is part of proper assessment. Risk management is the process that allows NICE inContact to balance the operational and economic costs associated with its controls to ensure optimal support of its mission to protect NICE inContact and its information assets.

Risk management includes:

1) Identify the risks
   a. Identify Company assets and information owners
   b. Identify Threats to those assets
   c. Identify vulnerabilities that might threaten those assets

2) Analyze and evaluate the risks
   a. Assess the business impact that might result from security failures
   b. Assess the likelihood of a security failure.
   c. Estimate the level of risk
   d. Determine whether the risks are acceptable

3) Identify and evaluate options for the mitigation of risk
   a. Transfer the risk
   b. Avoid the risk
   c. Apply controls to compensate for the risk
   d. Accept the risk

4) Select control objectives and controls for the mitigation of risks

Because no one control can achieve complete security, additional management action exists to monitor, evaluate and improve the effectiveness of security controls in the support of the Company objectives.

# Security Policies and Objectives

## *Security Policy*

Security policy provides direction and support for information and operational security in accordance with NICE inContact's requirements and any governing laws and regulations. All security policies are approved by the Company's Steering Committee, published and communicated to employees and any relevant external parties.

Information security policies are reviewed at least annually or more frequently if significant changes occur, to ensure their continuing suitability, adequacy, and effectiveness. Reviews include assessing opportunities for improvement of NICE inContact's information security policies and approach to managing information security in response to changes to NICE inContact's environment, new threats and risks, business circumstances, legal and policy implications, and technical environment.

### Security Objectives

- To ensure the protection of NICE inContact's business information, which includes the confidentiality, integrity, and availability of its data
- To safeguard information of its clients which NICE inContact has contractual obligations to protect
- To ensure that management and staff have an appropriate level of knowledge and awareness that will allow them to minimize the impact and occurrence of any security events
- To ensure that NICE inContact can continue its operational activities for itself and its customers in the event of any significant security event
- To comply with all state, federal, and international regulatory requirements in which NICE inContact is licensed to do business
- To create a safe, secure and productive working environment for employees while maximizing company profits

# Section 3: Assets

## Fixed and Intangible Asset Management

The purpose of asset management is to maintain the appropriate protection of the assets of NICE inContact and its clients. This requires all information assets and their owners be identified. Asset owners are responsible for classification of those assets and the maintenance of appropriate controls.

### Asset Management Objectives

- Ensure the cost-effective support of strategic decision making
- Gain control and ensure the security of the inventory
- Increase accountability to ensure compliance
- Enhance performance of assets and the life cycle management
- Protect the confidentiality, integrity, and availability of all information assets

**Assets**

- Products, designs, logos and collateral
- NICE inContact name and brand
- Employee Data
- Stockholder information
- Customer information

- Software technology and patents
- Capital assets
- Hardware
- Computer equipment
- Tangible assets
- Contracts and terms of agreement
- Financial data
- Email and any database of email archives
- Sales orders and customer and prospective customer database
- Billing systems, records and data necessary for billing
- All line of business software necessary to monitor, manage, control, process and bill
- Business plans
- Legal and regulatory information

# Section 4: Human Resources

## Human Resources Security

All employees, volunteers, contractors, and third-party users of NICE inContact information and information assets must understand their responsibilities and be deemed suitable for the roles they are considered for to reduce the risk of theft, fraud or misuse. Security responsibilities are addressed prior to employment in position job descriptions and any associated terms and conditions of employment. Where appropriate, all candidates for employment, volunteer work, contractors, and third-party users are adequately screened, according to the Company's Background Check Policy, especially for roles that require access to sensitive information. Management is responsible to ensure security is applied through an individual's employment with NICE inContact.

All employees undergo background checks. These checks include drug testing, employment verification, education verification, checking for felonies and misdemeanors in counties of residence for the past 7 years, and, if the candidate is in a position of cash responsibility, a credit check is also included.

NICE inContact requires all vendors, contractors and parties with access to NICE inContact or tenant data to undergo a vendor security assessment. This assessment includes requirements for background checks, security awareness training and access controls to ensure that our vendors and contractors have the capability of maintaining safeguards to protect such data.

Personnel are required to attend security awareness training upon hire. Employees are required to sign non-disclosure agreements and acknowledge receipt of training on company policies, Code of Ethics, and Customer Proprietary Network Information (CPNI). All employees receive appropriate security awareness training and additionally, regular updates on policies and procedures as relevant for their job function. NICE inContact's annual security awareness training includes acknowledgement and participation tracking. HIPAA and Medicare/Medicaid training is required and tracked for appropriate support staff.

Employee access, permissions, and job roles align with their job descriptions. All employees are reviewed for performance against goals and company policies at least annually.

Procedures exist to ensure an employee's, volunteer's, contractor's or third party's termination from NICE inContact is monitored and the return of all equipment and removal of all access rights are completed.

## *Human Resource Risk Assigned to Job Descriptions*

All NICE inContact employees, by the nature of the NICE inContact business model, interface on multiple levels with customer data.

While some data may be restricted based on need-to-know, an employee may at any time be required to service a customer at a level which may involve viewing customer data of whatever sensitivity classification. Within the NICE inContact corporate and customer domains, only appropriate employees have access to company and customer private, confidential, and sensitive data, as defined in the NICE inContact Data Classification Standard Operating Procedure.

That said, NICE inContact uses a risk ranking system (see matrix below) which rates employees high, moderate, and low regarding risk. Because of the NICE inContact business model, NICE inContact employees are rated at one of two risk levels, high or moderate.

Thus, Finance, Operations, Research and Design, Technical Support, Information Technology, Help Desk, Professional Services and Implementations are assigned a High-Risk rating. Sales, Human Resources, Collections, and all other staff are rated at Moderate Risk.

All members of the executive committee are also ranked at High Risk.

## Risk to Job Description Matrix

| Classification | Risk ranking | NICE inContact Personnel Permission Levels | Screening Criteria |
|---|---|---|---|
| Special-Sensitive | High | Admin | |
| | | | Access to sensitive Compliance and sensitive data (PRH) and all data below |
| | | | Access to any other intelligence-related Special Sensitive information or involvement in Top Secret Special Access Programs (SAP) |
| | | | Any other position the company management determines to be at a higher level than Critical-Sensitive due to special requirements from compliance organizations |
| Critical-Sensitive &<br>Non-critical-sensitive | Moderate | All other access | |
| | | | Access to non-compliance data, considered sensitive and critical (PRM) |
| | | | The adjudication, recommendation of adjudicative determinations, and/or granting of personnel security clearances |
| | | | Duty on personnel security boards |
| | | | Any other positions related to company security requiring the same degree of trust. |
| | | | Noncritical-Sensitive- Positions with the potential to cause damage to the company's security, up to and including damage at the significant or serious level. |
| | | | Noncritical-Sensitive- Positions with the potential to cause damage to the company's security, up to and including damage at the significant or serious level. |
| Non-critical-non-sensitive | Low | - N/A | |
| | | | N/A |
| | | | |
| | | | |

## Human Resource Security Objectives

NICE inContact will hire qualified ethical individuals capable of fulfilling the requirements of jobs and tasks while maintaining the confidentiality and integrity of NICE inContact and its customers' information.

# Section 5: Corporate Facilities

## Physical and Environmental Security

The objective of physical and environment security is to prevent unauthorized physical access, damage, theft, compromise, and interference to NICE inContact's information and facilities. Locations housing critical or sensitive information or information assets are secured with appropriate security barriers and entry controls. Facilities are physically protected from unauthorized access, damage and interference. Secure areas are protected by appropriate security entry controls to ensure that only authorized personnel are allowed access. Security is applied to off-site equipment. All equipment containing storage media is checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or release.

### *Physical and Environmental Security Objective*

NICE inContact will have and maintain offices and data centers that promote the security, ensure the integrity and facilitate the business continuity of its employees, data, services and business operations.

## NICE inContact Physical Security Requirements

1) 24x7 security utilizing live guards and or CCTV
2) Physical controls including card key access and pictured identification cards
3) Backup generator to provide protected power
4) UPS and battery protected systems
5) Redundant cooling systems
6) Environmental monitors are required for fire, smoke, heat and water
7) NICE inContact and NICE inContact authorized personnel are allowed access to the site
8) Managed access for authorized vendors and third parties
9) Redundant facilities for voice and data services
10) Redundant design for all real-time processing computer and storage systems
11) Fault tolerant design for network, storage and computing hardware systems
12) All systems and applications are monitored 24x7 for operational integrity, unauthorized activity, and performance
13) Floor to ceiling barrier
14) Locked equipment cages/cabinets

### *Physical Access Records*

Employees' physical access to NICE inContact facilities is logged, and these access logs are reviewed semi-annually.

NICE inContact maintains Data Center site visitor access records, and reviews these site visitor access records quarterly.

# Section 6: Operations

## Operations Management

### *Procedures for Managing Sensitive Information*

NICE inContact has implemented industry best practice measures for management of sensitive information. Such management includes storing and handling sensitive information measures so that customers can be assured that their data is managed securely. These practices are backed by policies and processes for those who manage the information.

- Policies outlining responsibilities and procedures specifying process for the secure management and operation of all information classifications, processing equipment and facilities have been established. The Computer Network Security Policy, System Maintenance Policy, Server Security Policy, Mobile Device Policy, are among the multiple policies mentioned at the beginning of this document that define the roles and responsibilities for secure management.
- Documented and implemented procedures for classifying, handling and storing information exist to protect information from unauthorized disclosure or misuse. Our Document Retention Process classifies data and indicates how long various classifications of data should be retained. Customer data is designated as sensitive.
- It is prohibited to use remote access technologies to copy, move, or store sensitive data on local hard drives and removable electronic media.
- It is important to note here that platform customers must classify their own data, and removing data from NICE inContact systems, while being enabled to do so by platform design, is determined by the customer.
- Policies and procedures establish the use of segregation where appropriate, to reduce the risk of negligent or deliberate system or information misuse.
- NICE inContact requires a minimum amount of data to perform its services. It requires a set of core data to process calls and contacts, including agent name, email address, and any phone numbers to dial, some set of skills, teams and campaign identification, and agent performance data. Data can

also include call recordings, and workforce optimization, if chosen. Tenants design their workflow with our professional services department to store only that data necessary to perform needed functions, and thus minimize risk.

- It is therefore noted here that tenants are responsible for limiting the amount to their data collected within the system, including limiting the time such information is retained to that reasonably necessary to accomplish such purpose, and limiting access to those persons who are reasonably required to know such information in order to accomplish such purpose, or to comply with state or federal record retention requirements.
- Media is controlled to prevent the modification, removal or loss of information and interruption to business activities.
- Media containing information is protected against unauthorized access, misuse or corruption during transportation beyond NICE inContact's physical boundaries.
- Employees are trained on what sensitive data consists of (PHI, ePHI, PII, PCI, and other designated data) and acknowledge this training, which includes that, in the ordinary course of business, they cannot keep, access, or transport records containing NICE inContact or tenant data outside of the business premises.
- Employees authorized in a support role may find it necessary to access customer data. Such access is always accompanied by a documented case within NICE inContact's Salesforce CRM, and this access includes a business reason, with notations of action taken.
- NICE inContact utilizes FIPS 140-2 compliant AES 256 encryption on its self-encrypting drive technology which secures data at rest.
- NICE inContact's WFO and QM provide encryption of call recordings. Transmission of information over unprotected networks utilizes strong encryption to protect data in transit.
- With each company policy comes a violation section, stating that "Gross negligence or willful disclosure leading to illicit exposure of NICE inContact information or customer information may result in prosecution for misdemeanor or felony resulting in fines, imprisonment, civil liability, and/or dismissal. Non-compliance with this policy can result in disciplinary action up to and including termination. In rare cases, a business case for non-compliance can be established; in all such cases, the non-compliance situation must be approved in advance through a risk acceptance process."

The scope of the security measures is reviewed at least annually and against material changes in business practices that may reasonably implicate the security or integrity of records containing tenant data.

### Portable Device Process

Portable devices such as laptops, and media storage devices such as flash drives, USB drives, thumb drives, jump drives, handhelds, tablets, smart phones, or zip drives have rules and procedures for their use in both transporting and storing information that achieves the business objective for their use and minimizes the risks associated with the loss, theft or misuse of those portable devices. All data identified as customer or client data, including, but not limited to, rates, contracts, emails, billing information and all data identified as private information kept on portable storage devices must be encrypted. Portable drive devices must meet the requirements of company policies and receive approval of the Help Desk and team management. Mobile Device Management (MDM) software and systems have been implemented to manage/enforce policies for company intelligent devices such as tablets and smart phones.

### Cloud Storage file storage services

NICE inContact Third party cloud storage may be utilized for storage. NICE inContact currently utilizes Amazon S3 for this storage.

### Operations Management Objective

The objective of the management of sensitive data is to ensure the confidentiality, integrity and availability of sensitive and critical data.

## Change Management

NICE inContact actively maintains a Change Control Management program based on a Change Management Policy. This policy provides the administration support for the overall change process including submission, validation and confirmation of the Change Control Request (CCR) from start to finish. A CCR is the form used to request a change to a production system. A Change Activities Board (CAB) convenes consisting of specific personnel responsible for various elements of the production environment and representing the best source of knowledge to evaluate each submission as it impacts various areas of the production environment.

This includes change management for the following:

- IT Project Requests
- Database Administration
- Billing Requests
- Network Operations Projects
- Production Systems Administration Projects
- Change Control Requests

The objectives, test plans and steps, impact and risk assessments, peer review and approvals (sign off by at least three designated change management personnel), and outcomes are considered within this regularly scheduled Change Activities Board meeting (corporate and production changes considered separately), Emergency changes follow similar approval with an attestation process.

The above elements are archived within the company CRM.

# Access Control

The access control covered in this section is referring to the underlying infrastructure of the NICE inContact platform, and not to the tenant application access.

Access to NICE inContact network and system infrastructure, (configuration information, hardware systems, configuration information, and information processing facilities), and business processes are controlled on the basis of business and security requirements and best practices. Procedures are implemented to control access rights and identifiers to information, information systems, and services based upon a need-to-know, and these requirements are typically defined in personnel job descriptions. Users are trained on responsibilities to maintain effective access controls, particularly regarding the use of passwords. Users are also trained on their responsibilities to ensure unattended equipment has appropriate protection. Access by terminated employees and employees who have changed jobs is promptly disabled. Steps are taken to restrict operating system access to authorized users. Protection is required according to the risks associated with using mobile computing and teleworking facilities.

## *Access Control Management Objectives*

1. Control access to Company and tenant information
2. Ensure that access controls meet Company business and Security requirements
3. Control access to NICE inContact data centers
4. Control access to NICE inContact's business processes
5. Access and identifier control rules comply with information authorization policies

## *Encourage Best Access Practices*

NICE inContact systems

1. Control system and network user access to information and information processing facilities. Access to tenant user password practices is provided such that tenant administrators can govern password policy.
2. Log user access.
3. Prevent information and information processing facilities from being exposed to possible loss or damage.
4. Prevent the theft of information and information facilities.

5. Identify types of accessible data. NICE inContact does this in a matrix, characterizing data from private high impact (PHI, ePHI, PII, PCI) to public low impact (non-sensitive, non-critical data). NICE inContact's employees are trained, and verified safeguards are practiced in accessing varied types of data, particularly with private, high impact data.
6. Ask authorized administrative users to help control access to NICE inContact information systems and information processing facilities.
7. Make authorized administrative users accountable for helping to control access to information and information processing facilities
8. Make company users aware of what they must do to securely assign and control access
9. Make company users aware of what they must do to protect passwords.
10. Make company users aware of what they must do to protect equipment.
11. Provide means within tenant software to securely assign and manage passwords, and provide training information on such access management
12. Reduce the risk of unauthorized access or damage to papers, media, and facilities by implementing a clear desk policy.
13. Preventing terminated employees from accessing records containing NICE inContact or tenant data by promptly terminating physical and electronic access to such records, including deactivating their passwords and user names.
14. Access to company network, systems and data is restricted to those that need to know, and assigned with the use of Active Directory policy.
15. Passwords are changed from vendor defaults.
16. Access to systems is according to policy, including those mentioned in Password Policies on page 24 below.

## *Control Access to Network Services*

1. Control access to internal networked services
2. Control access to external networked services
3. Control access by using the appropriate interfaces between the NICE inContact network and networks owned by other organizations
4. Control access by using the appropriate interfaces between the NICE inContact network and public networks

Control access to networks by using the appropriate authentication mechanisms for users and equipment

5. Control company user access to information services

## Control Access to Operating Systems

1. Prevent unauthorized access to NICE inContact operating systems
2. Restrict operating system access to authorized users
3. Establish ways of controlling access to operating systems
4. NICE inContact operating system access control methods comply with its access control policy
5. NICE inContact's access control methods are capable of recording successful and failed authentication attempts
6. NICE inContact's access control methods are capable of recording the use and abuse of special system privileges
7. NICE inContact's access control methods are capable of issuing alarms when system security policies are violated

## Control Access to Applications and Systems

1. Prevent unauthorized access to information held in NICE inContact application systems
2. Use security facilities to restrict logical access to NICE inContact application systems
3. Use security facilities to restrict logical access within NICE inContact application systems
4. Access to NICE inContact application systems and information is regulated by a formal business access control policy
5. Application systems control user access to application system functions
6. Application systems control user access to information held within application systems
7. Application systems can prevent utilities that are capable of overriding or bypassing system or application controls, from having unauthorized access
8. Application systems can prevent operating system software that is capable of overriding or bypassing controls, from having unauthorized access

9. Application systems can prevent malicious software that is capable of overriding or bypassing controls, from having unauthorized access
10. Application systems do not compromise the security of other interrelated application systems

### *Protect Mobile and Teleworking Facilities*

1. Information is protected when mobile computing facilities are being used
2. Security initiatives address the risks that mobile computing activities create
3. Mobile security initiatives address the risks associated with having to work in an unprotected environment
4. Information is protected when teleworking facilities are being used
5. Security initiatives address the risks that teleworking activities create
6. Teleworking sites are supported and protected

### *Password Policies*

NICE inContact maintains password policies that enable tracking of discreet users while mitigating risks associated with password storage, and brute force attacks.

Those password controls include rules for:

- Minimum password length and complexity: 8 characters, complexity enabled
- Change password upon initial login: Yes
- Maximum password life: 90 days
- Password history: Cannot duplicate 10 previous passwords
- Lockout policy: 5 failed attempts with 30 minute lockout
- Change of default vendor supplied passwords required

Log/Lock Policy: after 15 minutes of inactivity users will be either logged out of the application and/or screen saver policy will be activated. (with the exception of the Trainer AD group). VPN connections will be required to time out.

Details of NICE inContact password policies can be found within the NICE inContact Computer Network Security Policy.

## Password System Set-Up

All computers permanently or intermittently connected to NICE inContact networks must have password access/identifier controls. If the computers contain confidential or secret information, an extended user authentication system approved by the NICE inContact IT Department must be used.

Multi-user systems must employ user IDs and passwords unique to each user, and user privilege restriction mechanisms with privileges based on an individual's need to know. Network-connected, single-user systems must employ hardware or software controls approved by the IT Department that prevent unauthorized access. Unless an extended user authentication system is involved, computer and communication system access control must be achieved through fixed passwords unique to each individual user.

Access control to files, applications, databases, computers, networks, and other system resources through shared passwords or group passwords is prohibited.

Whenever system security has been compromised or if there is a reason to believe that it has been compromised, the involved system administrator must immediately change all involved privileged users.

Details of NICE inContact system set-up policies can be found within the NICE inContact Computer Network Security Policy.

## *Logon and Logoff Process*

All users must be positively identified prior to being able to use any NICE inContact multi-user computer or communications system resources. Positive identification for internal NICE inContact networks involves a user ID and unique, fixed password, both of which are unique to an individual user, or an extended user authentication system. Multi-factor authentication is used for remote administrative access to systems.

Details of NICE inContact system logon and logoff process can be found within the NICE inContact Computer Network Security Policy.

## *System Privileges*

### Limiting System Access

The computer and communications system privileges of all users, systems, and independently-operating programs such as agents, must be restricted based on the need-to-know, and based on restricting access to active users and active user accounts only. Privileges must not be extended unless a legitimate business-oriented need for such privileges exists.

Details of NICE inContact system access policies can be found within the NICE inContact Computer Network Security Policy.

### Process for Granting System Privileges

Requests for new user IDs and changed privileges must be in writing and approved by the user's manager before a system administrator fulfills these requests.

Non-NICE inContact employees must not be granted a user ID or be given privileges to use NICE inContact computers or networks unless the written approval of the Trust Office has been obtained.

Details of NICE inContact process for granting system privileges can be found within the NICE inContact Computer Network Security Policy.

### Process for Revoking System Access

Management must report all significant changes in worker duties or employment status promptly to the system administrators responsible for user IDs associated with the involved persons. For all terminations, the Human Resources department also must issue a notice of status change to all system administrators who might be responsible for a system on which the involved worker might have a user ID.

Details for the process for revoking system access can be found within the NICE inContact Computer Network Security Policy.

## Establishment of Unauthorized Access Paths

Employees, with the exception of Network Engineering, must not establish electronic bulletin boards, local area networks, FTP servers, web servers, modem connections to existing local area networks, or other multi-user systems for communicating information without the specific approval of the CTO. New types of real-time connections between two or more in-house computer systems must not be established unless such approval is obtained.

Similarly, NICE inContact security contains safeguards against unauthorized access paths into production using rogue access wireless networks. The NICE inContact Production network does not include a wireless network. The NICE inContact environment is scanned for rogue access wireless networks.

Details of NICE inContact process for granting system privileges can be found within the NICE inContact Computer Network Security Policy.

# Section 7: Information System (IS) Management

## Acquisition, Development, and Maintenance

Policies and procedures are employed to ensure the security of information systems. Encryption is used, where appropriate, to protect sensitive information at rest and in transit. Access to system files and program source code is controlled and information technology projects and support activities conducted in a secure manner. Technical vulnerability management is implemented.

The Computer Network Security Policy details the controls and processes for the storage and transmission of data, passwords and other sensitive items of information. It includes controls for when data should be encrypted, who should have access to data and how the data access level is determined.

NICE inContact information and users are divided between multiple network domains. Strict controls are in place to separate Corporate, Lab and Production domains. Those controls are specified and documented in the Computer Network Security Policy.

Additionally, standard operating procedures must be written and documented for all critical processes.

NICE inContact program and software development is maintained and controlled using a software development life cycle process known as Agile Development with Scrum. Team Foundation Server (TFS) is used to provide software source control, perform unit testing, track code reviews, and build projects for releasing new code in to production.

Secure coding and development processes are part of the development lifecycle and include a required rigorous annual training for secure coding practices, Quality Assurance testing for OWASP vulnerabilities and automated web application testing is performed. Steps are taken to proactively minimize vulnerabilities within the information system environments. Those steps include quarterly security scans, yearly penetration tests, internal scans, web application testing, monthly OS patch management, anti-virus and anti-malware software with timely application of updates and intrusion detection systems are in place in Corporate and Production networks to alert security personnel of threats and intrusions.

## *Information Security Incident Management Plan*

Information security incidents will be communicated in a manner allowing timely corrective action to be taken. Formal incident reporting and escalation procedures are established and communicated to all users. Responsibilities and procedures are established to handle information security incidents once they have been reported.

The Incident Management Process document describes how to identify a security incident, what actions must be taken to contain and remedy an information security incident, what information needs to be reported when a security incident occurs, when it must be reported and to whom it must be reported.

When an incident event is suspected, NICE inContact initiates its Incident Management Plan, summarized as follows:

- Preparation (pre-defining, documentation practices, training)
- Detection and Analysis (internal notification; identify level of impact, risk; isolate cause(s))
- Containment, Eradication, and Recovery (external notification, remediation)
- Post Incident Activity (root cause, lessons learned, preventative actions)

This cycle was formed around both NIST and SANS incident management guidelines.

## *Information Systems Management Objectives*

1. Produce high performance, reliable software and products that meet and exceed our customer's requirements
2. Ensure the security of our software, web services, databases and data against unauthorized use, intrusion, theft or malicious activities

3. Create a reliable time table for product and service releases
4. Create a product that is scalable, and easily maintained
5. Create a product that meets state, federal, industry and international regulatory and compliance requirements
6. Ensure the security and integrity of NICE inContact's valued software assets

## *Information Systems Management for Cloud Services*

NICE inContact may employ Cloud based services, IaaS, PaaS or SaaS models, to provide targeted services for its corporate and production requirements. Those services may include:

1. Billing
2. Human Resource Functions
3. Corporate Financial Services
4. Corporate Telecommunications Services
5. Production products and services such as ACD, IVR, reporting, Dialer, Workforce Optimization, and ECHO surveys
6. Backup functions. The NICE inContact application is a highly available, multi-site, highly available system, with a primary side backed up in real time by a secondary side. Database and configuration backup is then considered as integral to this architecture.

If Cloud services are utilized, they must not impair, or diminish the integrity, security, reliability or accessibility of those systems and customer data. Appropriate risk assessment will be performed. Regular audits and testing will be conducted in accordance with NICE inContact's existing practices and policies.

## *Data Management in a Cloud Environment*

Customers and prospective customers sometimes ask how their data is stored, and if data can be destroyed/disposed/sanitized if a tenant chooses to leave the NICE inContact services.

A tenant may leave and their data will be disposed according to terms with their contract.

Data for all customers is stored in a common database where customers are logically separated using unique business unit numbers. Details about this storage management may be obtained in the NICE inContact Technical FAQ in the Tenant Production Data Management section, which addresses NICE inContact data management.

# Section 8: Business Continuity

## Disaster Recovery and Business Continuity Management

The objective of business continuity management is to counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption. A disaster recovery and business continuity management process has been established to minimize the impact on NICE inContact and recover from loss of information assets to an acceptable level through a combination of preventive and recovery controls and extending to returning business to a normal level. A

A managed process exists for business continuity throughout the agency that addresses the information security requirements needed for NICE inContact business continuity.

The NICE inContact Disaster Recovery Business Continuity Plan (DR/BCP, rebranded Resiliency Event Management Plan, REMP) contains the following information and processes.

- DR/BC Strategy for updating
- Key Personnel
- External Contacts
- Notification Process
- Alerting, Escalations and Plan Invocation
- Notifications and Communications
- Financial and Legal Actions
- Disaster Recovery for Corporate Systems
- Disaster Recovery for Production Systems
- Damage Assessment for events
- Returning to Normal Business Operations
- Testing steps

### *Disaster Recovery and Business Continuity Objectives*

1) Ensure the real-time delivery of contact processing
2) Ensure the timely operation and servicing of non-real time products and services
3) Maintain the security of data centers, services, and information
4) Provide a safe and functional working environment for employees
5) Facilitate the continuity of employee performance of work and duties
6) Maintain continuity of communication and services to NICE inContact customers

7) Ensure the collection of necessary billing information and billing processes
8) Protect the investments of NICE inContact shareholders and owners
9) Meet and fulfill regulatory requirements for operations and services

# Section 9: Compliance

## Compliance

The design, operation, use, and management of information and information assets are subject to statutory, regulatory, and contractual security requirements. Compliance with legal requirements is necessary to avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements. Legal requirements include, but are not limited to: state, federal, and international requirements and regulations, contractual agreements, intellectual property rights, copyrights, and protection and privacy of personal information.

NICE inContact complies with:

- PCI
- FedRAMP (Federal Risk and Authorization Management Program)
- SOC 2 Type 2 (AT 101)
- HIPAA
- SOX 404 (from parent company, NICE, Ltd.)
- Privacy Shield (from parent company NICE, Ltd.)
- CPNI - Protecting Customer Information
- State and federal privacy requirements
- U.S. and international export controls
- State and federal laws governing telecommunications service providers
- European Union privacy requirements
- Red Flags Rule
- PUC & FCC telecom regulations
- NASDAQ
- SEC

Controls are established to maximize the effectiveness of the information systems audit process. During the audit process, controls will safeguard operational systems and tools to protect the integrity of the information and prevent misuse.

NICE inContact maintains both an Internal Audit department and a Trust Office department that perform:

- Quarterly audits
- Continuous monitoring
- Compliance (operational and financial)
- Coordination of external audits
- Creation, review and auditing of compliance and security procedures
    - Standard Operations Procedures
    - Company Policies
    - Best Practices
- Reporting
- DR and Incident Response (IR) planning and testing
- Quarterly internal and external vulnerability scans
- Annual penetration testing
- Security training
- Product security review and assessment
- Vendor security assessments
- Dedicated compliance personnel

## PCI

NICE inContact tests against the PCI Council's Data Security Standards (DSS) controls. NICE inContact currently tests for the previous full year.

NICE inContact offers both an Attestation of Compliance (AOC) and a PCI Responsibility Matrix to customers with contract and to prospective customers with a non-disclosure agreement (NDA).

## SOC 2

NICE inContact tests against the  Service Organization Controls (SOC) from the AICPA SOC reporting framework, and issues a AT 101 SOC 2 report (SOC 2 Type II).  NICE inContact currently tests for the previous full year. These tests are performed on a schedule appropriate to expiration. If there is a gap between when this assertion expires and the issuing of the next report, a bridge letter can be made available to customers.

## *HIPAA*

NICE inContact policy dictates the company will sign a Business Associates Agreement (BAA) with a customer that requires such from a vendor, whether that customer themselves is a Covered Entity (CE) or a Business Associate (BA). Such an agreement will cover the BAA requirements within the Federal Regulations, and observe HIPAA security safeguards, including the following:

- Technical Safeguards
  - RBAC, unique identity, as well as VPN encryption requirements
  - Logging and monitoring
  - Redundancy and Backups
  - Secure Data storage, transport, portable media encryption
  - IDS/IPS, AV/Malware, and port restrictions
  - Implementation practices converted to process
  - Patching
  - Secure development lifecycle, testing and reviews
  - Change control
- Training Safeguards
  - Annual security awareness
  - Role based HIPAA training
- Vendor Assessment Safeguards
  - Vendor security assessment
  - Restricted and monitored vendor access
- Administrative Safeguards
  - Computer Security and other policies mentioned earlier in this document
  - Risk management
  - Resiliency and incident management plans and tests
  - Security and audit roles defined
  - Hiring practices, including third party background checks
  - Non-disclose, non-compete agreements w. employees and prospective customers
  - User audits
  - Business Associate proforma with legal staff review
  - Dedicated Security team

NICE inContact requires vendors who will themselves bundle PHI to sign a BAA with NICE inContact.

## *FedRAMP*

NICE inContact is commited to meet the needs of our customers, including government. NICE inContact provides an environment that has been assessed by a 3PAO against the Federal Risk and Authorization Management Program (FedRAMP) marketspace. Based upon that assessment, we are able to offer this environment to agencies that would like that level of assessment. The FedRAMP environment operates under a separate set of policies and procedures, and is aligned with NIST 800-53. NICE inContact can now offer its world-class NICE inContact CXone™ ominchannel customer experience to government contact centers upon approval.

## Verifying NICE inContact Vulnerability Surfaces

NICE inContact performs security testing of its Cloud threat surfaces. Regular vulnerability and penetration tests assure that NICE inContact's security protection measures follow industry best practices and counter the most current threats.

These tests are performed by qualified internal and external assessors that are certified in their fields.

Quarterly vulnerability testing, as required by regulation, is performed on information assets evaluated as in-scope based on these assets' potential risk as points of potential attack. Using accepted industry tools backed by qualified external assessors assures that threats are discovered and mediated quickly. Vulnerability tests are designed to review current industry lists of vulnerabilities. Additional scans may be performed as required and determined necessary.

Using an independent penetration company, penetration testing at least yearly is performed, as required by regulations and as deemed necessary. NICE inContact also has staff trained in penetration testing and security assessment. Testing is based on current industry lists of penetration vulnerabilities compared against identifiable NICE inContact vulnerabilities to determine exploitability of any identified vulnerabilities. Plans are made to conduct such testing and follow-up monitoring at least once a year. Penetration testing will include the following tests:

- Black box testing of the in scope external network.
- Automated testing and scanning of the in scope external network
- Privileged access authorization to information system components will be granted for internal application testing.
- Testing will be performed to validate intrusion detection and incident response processes.

In every case, a change control management process evaluates the risk and impact to the business prior to the authorization of the vulnerability scan or penetration test.

## Compliance Objectives

NICE inContact will maintain state, federal, industry, and international regulatory and compliance requirements that are necessary for its operations as a SaaS provider of hosted contact center services. Additionally, NICE inContact will provide solutions that fulfill its customers' compliance requirements.

## eDiscovery

Within the NICE inContact Data Retention Policy there is a 7 year requirement for Litigation data after settlement as well as retention for other classes of documents that may be used for forensic investigation. NICE inContact also maintains a Code of Ethics through its parent company NICE that commits employees to cooperate with investigations.

# Section 10: Common Controls

## Common Controls

Common controls are security controls that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application that the control protects.

### *NICE inContact Common Controls*

- Backups
- Change Management
- NICE Code of Ethics
- Code Release Procedures
- Company Handbook
- Computer Network Security Policies
- Continuous Network Monitoring and Alerting
- CPNI Training
- Critical Vendor Policy
- Cryptographic Key Management Policies
- Data Center Design Policies (Multiple Data Centers, Access Control, Power, Cooling, Redundancy, Fire Protection)
- Data Retention Policy
- Disaster Recovery Plan (REMP) document
- Data encryption
- Executive Committee
- Firewalls
- IDS/IPS
- Hardware Retirement Policies
- Hiring Policy
- Internal Audits

- Job Descriptions
- Logging and Auditing
- Maintenance and Data Center Work Policies
- Malicious Code Protection (Anti-Virus, Anti-Malware, Patch Management)
- Network Time and Time Stamps
- Password and User Permissions Policies
- Multi-Factor Authentication
- Penetration Tests
- Physical Access and Visitor Control Policies
- CCTV
- QA Testing
- Risk Assessment Committee
- Security Awareness Training
- Steering Committee
- Termination Policy
- Vulnerability Scans

# Section 11: Approval

## Approval

Chief Security Officer

Date

VP Strategy and Architecture

Date

Henry St. Andre

Director of Trust

9/19/17

Date

NICE · inContact

# Technical FAQ

## Cloud Services Redundancy and Fault Tolerance Architecture

**V. 5.57**

**June 2018**

This document includes proprietary information of NICE inContact, Inc. This document is for information purposes only and is subject to change without notice. The information contained in this document represents the current view of NICE inContact, Inc., on the issues discussed as of the date published and does not constitute legal advice, representation, warranty or guarantee regarding the products or services described or anyone's ability to comply with applicable regulatory requirements.

## Table of Contents

## Table of Figures

# Executive Summary

NICE inContact leverages a global foot print to provide contact center cloud interaction services around the world. The NICE inContact platforms are comprised of physical plant, data services, computer networks, storage systems, applications and reporting systems. Ensuring platform performance, fault tolerance and operational redundancy requires a layered approach. In this paper we discuss the controls and architecture that NICE inContact uses to provide availability to customers, an infrastructure that allows for NICE inContact's 99.99% availability (industry best) SLA to its customers on Automatic Call Distribution (ACD):

- Diverse, geographically redundant NICE inContact data centers have been designed to provide protection against natural and man-made disasters. Disaster strategy and planning assures protection against loss of systems, data, and utilities.

- The NICE inContact computer and data networks are secure, redundant and scalable by virtue of hardware selection, architectural design, and selected service providers.
- NICE inContact's customer data integrity is protected by redundant databases using real-time replication, encryption of data at rest, HTTPS, SFTP, and high performance hardware storage systems.
- In the United States, NICE inContact is a full service telecommunications company, in addition to being a provider of SaaS solutions. The Company is able to provide a full range of Toll Free, Dedicated, VoIP, Long Distance, and Local DID services. The NICE inContact telecommunications network uses multiple leading national service providers to maintain a redundant, scalable network that can meet the calling demands of small, medium and large call centers.
- NICE inContact's hosted applications are developed with secure coding practices using Microsoft Team Foundation Server (TFS) for code management, and these developed applications are designed to ensure fault tolerance and survivability of calls and services.
- NICE inContact's internal and external threat surfaces are monitored by periodic, industry recognized, third party vulnerability and penetration tests and methodologies. Industry leading intrusion detection and protection technologies are employed through NICE inContact's routers, firewalls, and switches.
- Network management and monitoring is provided by the Network Operations Center, or NOC which is staffed 7 x 24 x 365. NICE inContact monitors the physical environment, hardware, network, and applications using visual, audible and email alerts. Trained network analysts are able to identify, correct and escalate issues that impact SaaS services.
- Security and compliance infrastructures and industry standard practices are in place such as:
    - SOC 2 Type 2 (AICPA) audited data centers
    - PCI DSS compliance
    - Perform HITRUST (HIPAA) by means of SOC 2 Type 1
    - GDPR observance: verification (Article 15), rectification (Article 16), erasure (Article 17), restriction (Article 18), or portability (Article 19).
    - NICE Privacy Shield Certification
    - Red Flag Rule compliance
    - Change control policies and management
    - Regular and timely security patch management,
    - Disaster recovery/business continuity (resiliency event management) planning

  - Regular security awareness and policy training

  These and other practices combine to provide transparency into NICE inContact's regulatory compliance and service integrity.

- As the world's current leading provider of hosted contact services, and with data centers in the USA and Europe as well as Australia and Singapore, NICE inContact enables customers to have global reach.
- NICE inContact collaborates with other significant cloud providers to be at the forefront of strategies to assure cloud integrity.
- Recognizing early the customer's need for Cloud Security, in 2009, NICE inContact established its Trust Office to assure customer transparency into - and integrity of - security, performance, and reliability.
- NICE inContact builds disaster recovery (resiliency) into its data centers and software, and maintains both a Resiliency Event Management Plan (DR/BC) and Incident Management Plan. NICE inContact utilizes multiple sets of redundant services, systems and hardware. Data integrity processes include disaster recovery tests, backups, and real time data replication.
- All systems are monitored at multiple levels, including logical, functional, and environmental. Hardware and application status and all such monitoring is fed back to the NICE inContact 24x7x365 Network Operation Center. System logs are monitored through Security Information and Event Monitoring (SIEM) applications. Additionally, ACD applications are designed to allow for automatic recovery and failover of services. In many cases, systems can even fail transparently to the user.

Finally, the ability of these systems to function at the cluster level of integrity is tested periodically in a process that routes all cluster contact processing from one data center to the other, effectively validating the ability for those systems to function independently at the cluster level in the event of a data center outage.

This document includes proprietary information of NICE inContact, Inc. This document is for information purposes only and is subject to change without notice. The information contained in this document represents the current view of NICE inContact, Inc., on the issues discussed as of the date published and does not constitute legal advice, representation, warranty or guarantee regarding the products or services described or anyone's ability to comply with applicable regulatory requirements.

# Data Centers and Physical Security

Confidentiality, Integrity and Availability (CIA), the Security Triad, are integral architectural considerations when NICE inContact selects, designs and builds out its data centers. Observance of these principles begins with the physical structure that house NICE inContact services. In both the United States, Germany, and Australia, NICE inContact utilizes paired, geographically diverse data centers, housed in carrier-grade facilities. POP sites for system enhancements are also maintained in Singapore and the Philippines. These facilities were selected for their ability to provide access to leading carriers, assurance of Data Center tier standards, and secure physical controls.

## United States

### Los Angeles

Los Angeles – Coresite at Alameda (LA2):

- Described as one of the preeminent points for telecommunication and network interconnection
- 7x24x365 security using live guards and CCTV
- Double mantrap entries, locked cabinets/cages
- Card key access is used to control access to elevators, floors and data center
- Climate control
- All access to the NICE inContact resources within facility is controlled/managed by NICE inContact
- Building-supplied backup generators plus NICE inContact UPS and battery protection
- Fully functional redundant cooling systems
- Redundant and multiple fiber optic entrance facilities and Gig-E and 10 Gig interfaces provide access to ISP's and telecom service providers
- Fire Suppression
- SOC 2 and PCI Assertions (NICE inContact authorized to redistribute)
- http://www.coresite.com/resources/slk-mkt-la

**Figure 1 - Alameda Coresite - NICE inContact Cage Area and Coresite Security Monitoring**

## Dallas:

Dallas – Level 3 colocation facility

- Level 3 is one of the largest colocation providers in the world
- 7 x 24 CCTV
- Man traps and card key access controls, locked cabinets/cages
- Fully protected power including backup generator
- Climate control
- NICE inContact maintains separate locked equipment cabinets within the facility.
- Redundant and multiple fiber optic entrance facilities and Gig-E and 10 Gig interfaces provide access to ISP's and telecom service providers.
- Fire Suppression
- SOC 2 and PCI Assertions (NICE inContact not authorized to redistribute)

http://www.level3.com/en/resource-library/wp-high-density-data-centers/

Figure 2 – Dallas Level 3 NICE inContact Locked Cabinets

# Europe

## Frankfurt and Munich

Frankfurt/Munich – Equinix colocation facilities:

In 2011, NICE inContact opened its first full service data centers in the European Union. Our selection of Equinix demonstrates NICE inContact's commitment to performance and reliability. Equinix provides state-of-the-art services. A short list of their features is provided, along with a reference where additional details can be obtained.

- ISO 9001, 27001, SOC 1,2, PCI (NICE inContact is not authorized to re-distribute)
- 3 Stages of Access – site entry door, reception, and card access
- N+1 Power systems
- Robust HVAC system to provide stable airflow, temperature and humidity, with minimum N+1 redundancy for all major equipment
- 7 x 24 x 365 Security
- CCTV
- Fire Suppression

http://www.equinix.com/en_US/platform-equinix/platform-advantages/ibx-data-centers/

This document includes proprietary information of NICE inContact, Inc. This document is for information purposes only and is subject to change without notice. The information contained in this document represents the current view of NICE inContact, Inc., on the issues discussed as of the date published and does not constitute legal advice, representation, warranty or guarantee regarding the products or services described or anyone's ability to comply with applicable regulatory requirements.

Figure 3 - Germany Equinix NICE inContact Locked Cage

# Australia

## Melbourne and Sydney

In 2018, NICE inContact opened its first full service in Equinix data centers in Melbourne and Sydney, Australia. Equinix was again selected as our data center based on their commitment to security and reliability. Equinix provides state-of-the-art services. A short list of their features is provided, along with a reference where additional details can be obtained.

- ISO 9001, 27001, SOC 1,2, PCI (NICE inContact is not authorized to re-distribute)
- 3 Stages of Access – site entry door, reception, and card access
- N+1 Power systems
- Robust HVAC system to provide stable airflow, temperature and humidity, with minimum N+1 redundancy for all major equipment
- 24 x 7 x 365 Security
- CCTV
- Fire Suppression

This document includes proprietary information of NICE inContact, Inc. This document is for information purposes only and is subject to change without notice. The information contained in this document represents the current view of NICE inContact, Inc., on the issues discussed as of the date published and does not constitute legal advice, representation, warranty or guarantee regarding the products or services described or anyone's ability to comply with applicable regulatory requirements.

Figure 4 - Sydney Locked Cages and Cabinets

# Telecom and Global Data Network Architecture

- NICE inContact connects to its service providers using redundant, high capacity 10 Gig, GigE and FastE interfaces as well as Time Division Multiplexed (TDM) services (DS1, DS3, OC3, OC12). TDM services utilize redundant fiber optic entrance facilities.
- NICE inContact's traditional telecom network utilizes paired SS7 links and redundant SS7 proxies for call control in each data center to assure fault tolerance and redundancy.
- NICE InContact's VoIP network deploys VoIP, utilizing redundant SIP trunks to its carriers. Each SIP carrier is provisioned in each paired data center, with Los Angeles/Dallas in the USA, Frankfurt/ Munich in Europe and Melbourne/Sydney providing VoIP network redundancy.
- All SIP services are processed through redundant, fault tolerant Session Border Controllers or System Border Controls (SBCs) deployed in each data center. (An SBC is functionally a VoIP firewall.)
- NICE inContact utilizes Tier 1 national carriers to provide diverse, toll free (TF) routes and long distance termination routes.
- All telecom and Internet services are provisioned as redundant pairs or groups of services.
- In the USA, services are designed to allow NICE inContact to process telecom services including Toll Frees (TF)s, Direct Inward Dials (DID)s, international TFs (ITF)s, international DIDs and long distance calls via each of its USA data centers.
- In Europe, services are designed to allow NICE inContact to process telecom services, including ITFS, international DIDs and long distance calls from each of its data centers

This document includes proprietary information of NICE inContact, Inc. This document is for information purposes only and is subject to change without notice. The information contained in this document represents the current view of NICE inContact, Inc., on the issues discussed as of the date published and does not constitute legal advice, representation, warranty or guarantee regarding the products or services described or anyone's ability to comply with applicable regulatory requirements.

- In the USA, NICE inContact is a full service RESPORG, allowing us to route and reroute TF numbers between different carriers. This distributes traffic amongst multiple carriers and reduces risks and impact associated with the loss of a single carrier.
- NICE inContact has deployed a redundant Sonus Softswitch and SBC to each of its Los Angeles and Dallas data centers.
- NICE inContact has deployed a redundant Sonus Softswitch and SBC to each of its Frankfurt and Munich data centers.
- NICE inContact has deployed a redundant Sonus Softswitch and SBC to each of its Melbourne and Sydney data centers.
- The NICE inContact telecom and Internet networks are designed to detect carrier and component failures and automatically redirect new voice and data traffic to redundant, alternate facilities.

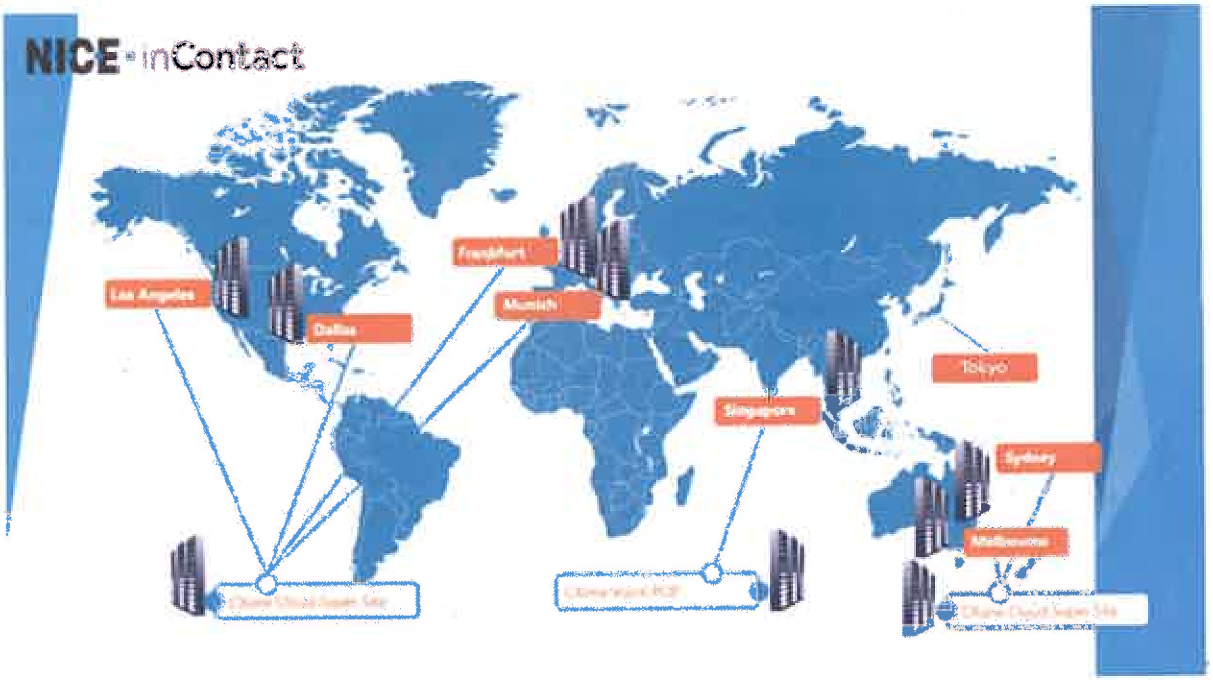


Figure 5 - NICE inContact's World Pop Site Coverage

# Data Network - Design and Redundancy

NICE inContact's data network is designed around Brocade, Cisco and Palo Alto technology for infrastructure switches, routers and firewalls. All network equipment is designed with high availability, high capacity, fault tolerance, redundancy and scalability. The network diagrams provided demonstrate the redundant architecture and design:

- Multiple redundant leading ISPs using Gig-E interfaces
- Redundant edge routers, load balancers, Firewalls, and ELB (Amazon space)
- USA EU, and Australia data centers incorporate redundant BGP design

- BGP peering to automatically redirect internet traffic around problems

Fault Tolerant & Redundant Internet Connection Model

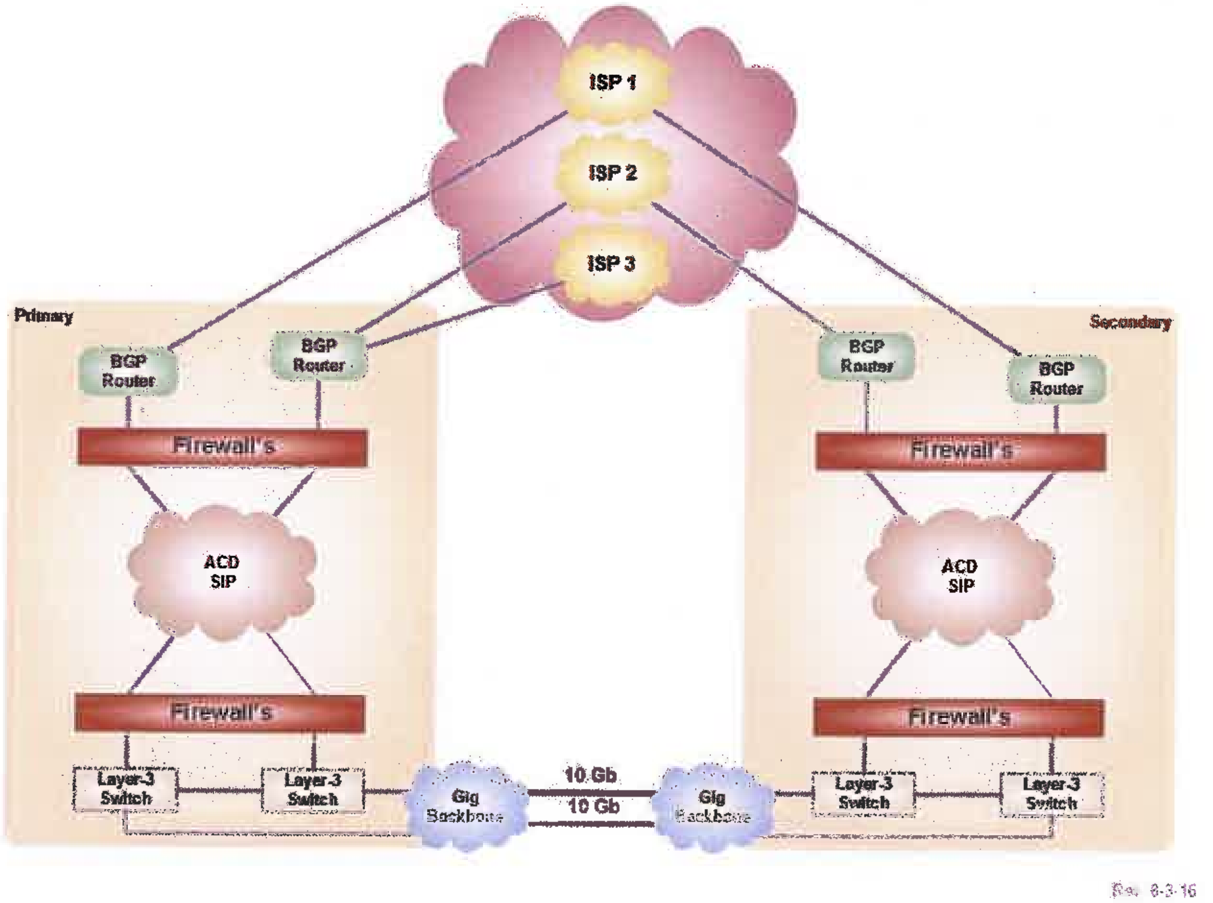


**Figure 6 - Redundant Connection Model**

- Redundant 10 Gb connected firewalls
- Intelligent Next Gen firewalls incorporate intrusion detection, intrusion protection and malware detection capabilities

This document includes proprietary information of NICE inContact, Inc. This document is for information purposes only and is subject to change without notice. The information contained in this document represents the current view of NICE inContact, Inc., on the issues discussed as of the date published and does not constitute legal advice, representation, warranty or guarantee regarding the products or services described or anyone's ability to comply with applicable regulatory requirements.

- Firewall protected DMZs for customer facing applications
- A segmented internal network protects production services
- Layer 3 redundant, GigE/10Gig Layer 3 switches drive the internal production network
- USA and European data centers utilize dual 10 Gig and GigE services creating a redundant, high performance, high capacity backbone between the pairs, i.e. Los Angeles to Dallas, Frankfurt to Munich, Sydney to Melbourne, and between AWS availability zones
- Data services are designed for automatic fail-over and recovery
- High capacity MPLS network bridging its data centers in the USA, Europe. and providing connections to its voice POPs in Singpore and the Philippines.

This document includes proprietary information of NICE inContact, Inc. This document is for information purposes only and is subject to change without notice. The information contained in this document represents the current view of NICE inContact, Inc., on the issues discussed as of the date published and does not constitute legal advice, representation, warranty or guarantee regarding the products or services described or anyone's ability to comply with applicable regulatory requirements.

## World-Class Network Topology

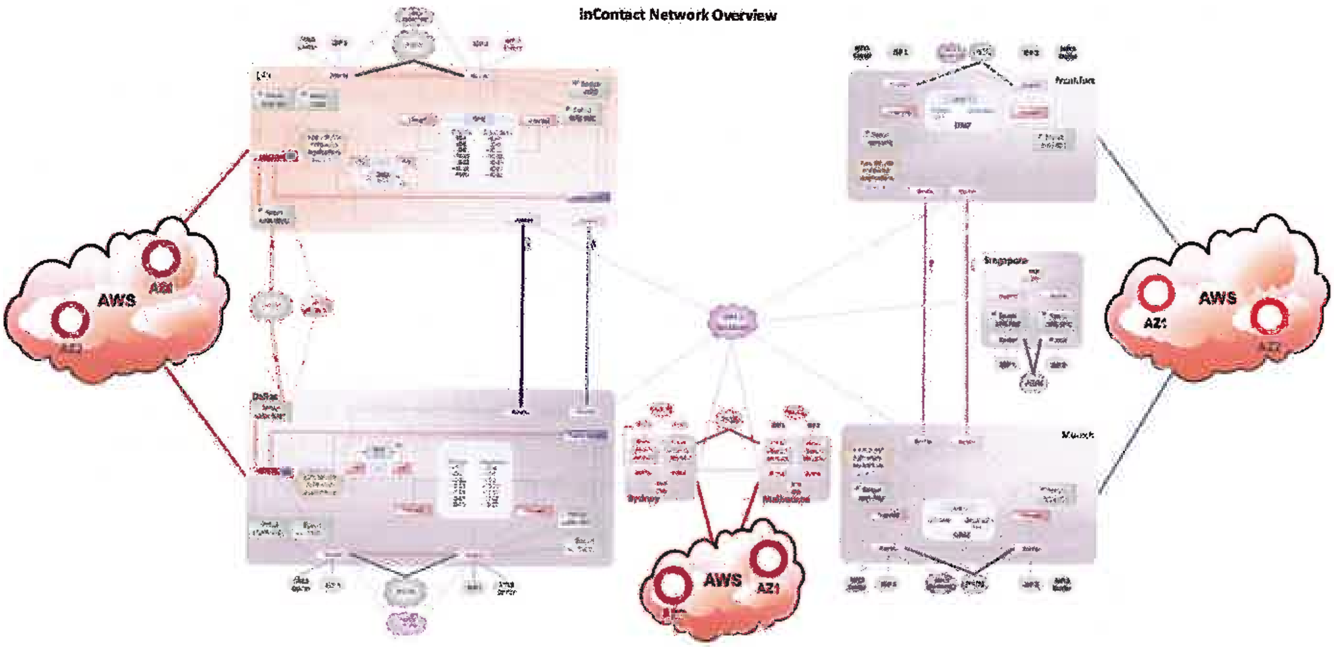


Figure 7 - NICE inContact Worldwide IP-TDM Network

## Tenant Production Data Management

Customers and prospective customers sometimes ask how their data is stored, and if data can be destroyed/disposed/sanitized if a tenant chooses to leave the NICE inContact services.

A tenant may discontinue services and their data will be disposed according to terms with their contract.

Data for all customers is stored in a common database where customers are logically separated using unique business unit numbers. The data stores are on Hewlett Packard (HP) Storage Area Network (SAN) systems, specifically, HP 3PAR. These are multi-terabyte systems with hundreds of drives using RAID 10, and are encrypted drives. Any tenant data is distributed across multiple drives. There is no single drive that one would sanitize for an individual tenant.

The SAN is maintained by Hewlett Packard (HP). If drives fail, they usually fail one or two at a time. HP comes on-site and replaces the drive. NICE inContact contracts with HP to securely process failed drives which are securely returned to HP. In the unusual case where an entire SAN might be retired, thus containing a functioning set of data on a complete system, that data would be wiped (disposed of) before the SAN was retired.

Also, operationally at the desktop level, (which by policy and review doesn't contain tenant data) and at a few discrete server levels, where there might be discrete drives, NICE inContact

This document includes proprietary information of NICE inContact, Inc. This document is for information purposes only and is subject to change without notice. The information contained in this document represents the current view of NICE inContact, Inc., on the issues discussed as of the date published and does not constitute legal advice, representation, warranty or guarantee regarding the products or services described or anyone's ability to comply with applicable regulatory requirements.

operations does perform physical drive destruction using a bonded company to shred the drives.

The HP Drives are augmented with Pure Storage solid state technology which incorporates the same drive-level encryption.

Call recordings on ACD are managed using a proprietary file management system. When a call recording is deleted, that data segment is marked so that the space the recording uses is now available for re-use and will periodically be overwritten by a new call from a different BU. There is, however, no folder that contains a single tenant's discrete call recordings. And the call recordings are not identified in any fashion on the drive systems that would associate them with a single tenant. All such location of data is kept in the proprietary database that identifies those call recordings by their unique business unit.

Finally, as it relates to data sanitizing -- it is technically feasible to CLEAR (NIST Term) data from the databases, such as contact history/meta data – this could be done at contract term or might occur on periodic record purge. This process is determined by customer requirement, and therefore can be clarified by an assigned sales engineer in conjunction with NICE inContact Professional Services.

## AWS S3 Storage

NICE inContact offers services within the AWS cloud S3 storage structure within the AWS Region US-West-2 (Oregon), the US-EAST-1 (N. Virginia) and Asia-Pacific Southeast-2 (Australia). A diagram of these services is offered in the AWS S3 Storage Diagram below

Currently this storage includes SMS Messaging requests, email, ACD call recordings, and WFO call recordings.

AWS is responsible for all physical security controls. These practices are detailed in the aforementioned AWS Security Fundamentals training.

- Escort - All visitors are signed in and continually escorted by authorized staff. All physical access is routinely logged and audited.
- Security Staff and Surveillance - Professional security staff use video surveillance, intrusion detection systems, and other electronic means
- Two-factor Authentication - Staff must pass two-factor at a minimum of two times to access data center floors. Identification is required. Access and information is only provided to those who have a legitimate business need.
- Building - AWS data centers are housed in nondescript facilities. Tenant visitors are not welcomed.
- Perimeter and Entry - Physical access is strictly controlled both at the perimeter and at the building ingress points.
- ISO 9001, 27001, SOC 1,2, PCI (NICE inContact is not authorized to re-distribute)

This document includes proprietary information of NICE inContact, Inc. This document is for information purposes only and is subject to change without notice. The information contained in this document represents the current view of NICE inContact, Inc., on the issues discussed as of the date published and does not constitute legal advice, representation, warranty or guarantee regarding the products or services described or anyone's ability to comply with applicable regulatory requirements.

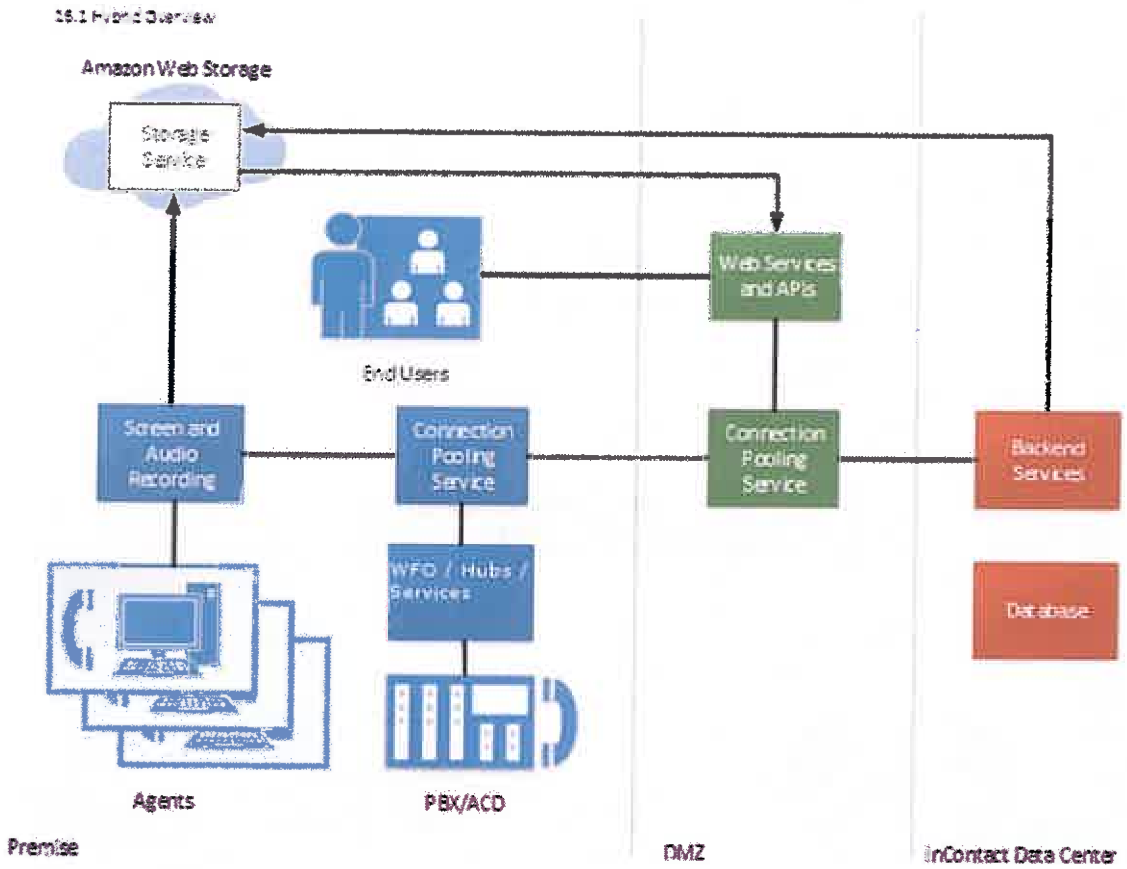


**Figure 6 – AWS S3 WFO Centric Topology Overview**

## AWS S3 Storage Diagram

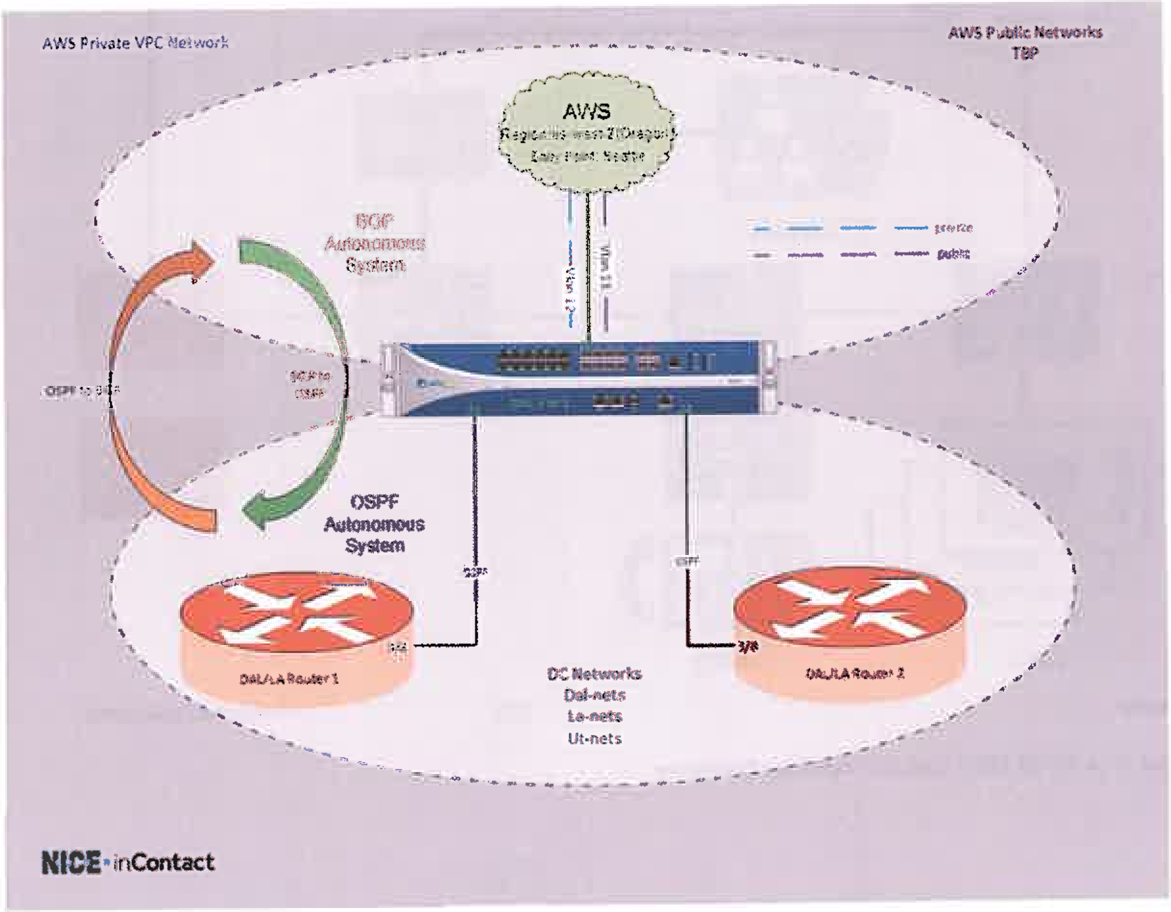


Figure 8 - AWS S3 Connection to LA and DAL Data Centers

- AWS utilizes dual 10 Gig and GigE services creating a redundant, high performance, high capacity backbone from AWS to Los Angeles and Dallas (not Frankfurt and Munich)
- Data services are designed for automatic fail-over and recovery
- A customer may request the NICE inContact whitepaper "Amazon S3 Storage" to see the security features of this Amazon storage

## AWS Data Encryption with KMS

NICE inContact utilizes Amazon AWS S3 data storage services, which encrypts at a file level, and uses AWS Key Management Service (KMS) to protect encryption keys.

This document includes proprietary information of NICE inContact, Inc. This document is for information purposes only and is subject to change without notice. The information contained in this document represents the current view of NICE inContact, Inc., on the issues discussed as of the date published and does not constitute legal advice, representation, warranty or guarantee regarding the products or services described or anyone's ability to comply with applicable regulatory requirements.

AWS Key Management Service (AWS KMS) provides cryptographic keys and operations scaled for the cloud. AWS KMS keys and functionality are used by other AWS cloud services, and you can use them to protect user data in your applications.

AWS KMS

- provides a simple web services interface in the AWS
  - Management Console,
  - Command Line Interface, and
  - RESTful APIs

This interfaced is used to access an elastic, multi-tenant, hardened security appliance (HSA).

This is an interface that can be used to generate and manage cryptographic keys and operate as a cryptographic service provider for protecting data. It offers traditional key management services integrated with AWS services to provide a consistent view of customers' keys across AWS, with centralized management and auditing.

Below is a flow diagram for AWS KMS key management for S3

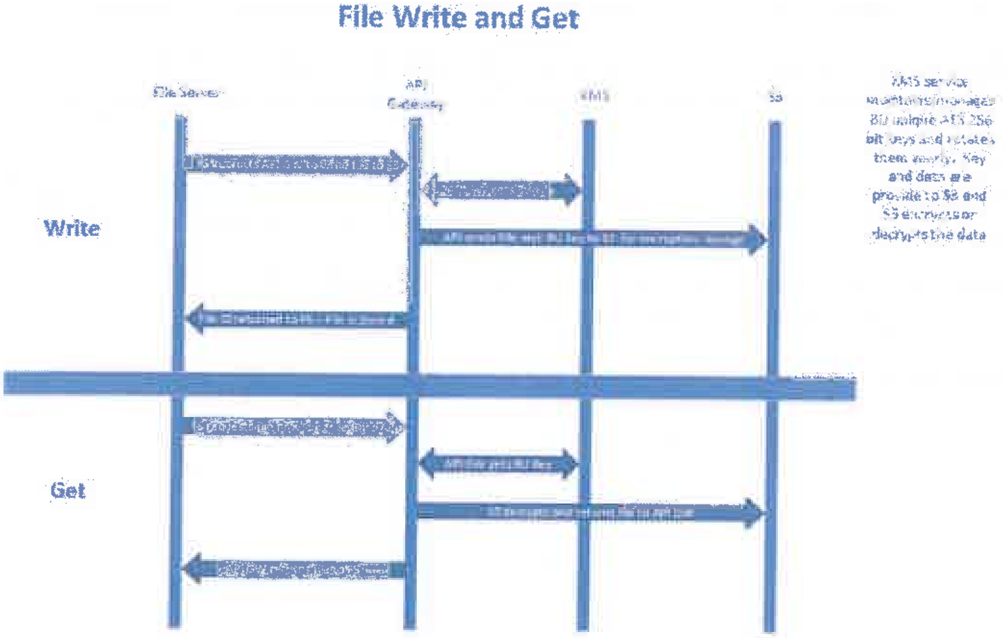

File Write and Get
File Server
API Gateway
KMS
S3
KMS service maintains/manages 8U unique AES 256 bit keys and rotates them yearly. Key and data are provide to S3 and S3 encrypts or decrypts the data
Write
Get

Figure 9 - AWS Key Management Flow

More detail is available here: [https://d0.awsstatic.com/whitepapers/KMS-Cryptographic-Details.pdf](https://d0.awsstatic.com/whitepapers/KMS-Cryptographic-Details.pdf)

This document includes proprietary information of NICE inContact, Inc. This document is for information purposes only and is subject to change without notice. The information contained in this document represents the current view of NICE inContact, Inc., on the issues discussed as of the date published and does not constitute legal advice, representation, warranty or guarantee regarding the products or services described or anyone's ability to comply with applicable regulatory requirements.

# Computer Hardware

- The NICE inContact services are housed on Hewlett-Packard (HP) Carrier Grade infrastructure , in most cases using blade chassis architecture. HP manufactures platforms are Network Equipment Building System (NEBS) and European Telecommunications Standards Institute (ETSI) certified. The public cloud services are housed on hardened images within Amazon.
- Encrypted SAN and solid state storage and Encrypted Elastic Block Storage (EBS) within Amazon for S3 and Glacier systems provide data integrity and scalability.
- NICE inContact maintains a Disaster Recovery/Resiliency Event Management Plan that includes full vendor hardware support agreements for all critical systems.

# VoIP/SIP Network

NICE inContact is committed to provide carrier-grade VoIP services.

- VoIP services are provisioned over redundant interfaces.
- NICE inContact uses paired redundant Session Border Controls (SBCs) in each data center. An SBC is a SIP firewall and is specifically designed to manage SIP IP sessions.
- VoIP carrier connections are implemented in paired peering relationships that allow traffic to be routed to or from either of our Data Centers pairs in the USA, Europe, or Australia.
- The VoIP network also supports SIP agents and SIP trunking to provide a reliable method to connect agents and customer voice services to NICE inContact services.
- SIP trunking can be provisioned over MPLS to ensure quality of service and provide a security for the transport of voice services.
- VPN tunnels can be deployed to secure call signaling and RTP payloads.

# NICE inContact ACD Application Design

The NICE inContact hosted contact center application is designed to be able to process contacts even in the presence of external or internal problems, including the following:

- Redundant ACD servers allow ACD system failover and recovery.
- Multiple redundant voice processing servers provide scaling and automatic service recovery.
- Self-testing applications that detect problems and automatically switch traffic to redundant applications.
- Multiple redundant IIS servers support web applications, and are enhanced by Layer 7 load balancing switches. Layer 7 switching provides load balancing as well as system recovery in the event of a web server problem.

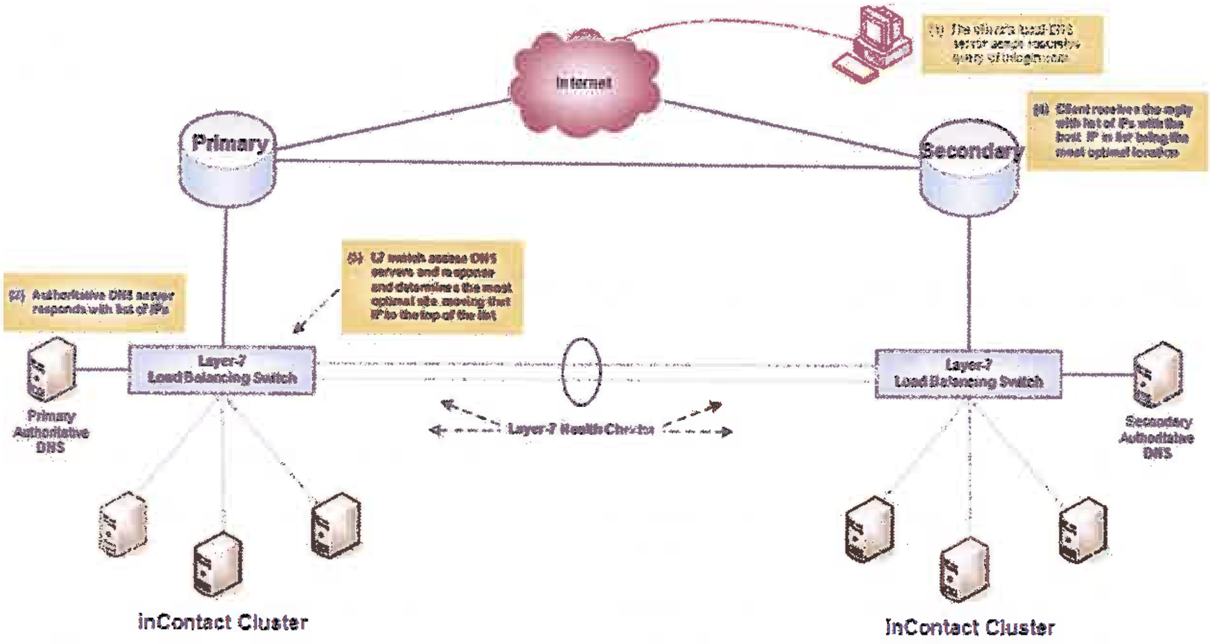

Internet
(1) The client's local DNS server sends recursive query of
(4) Client receives the reply with list of IPs with the first IP in list being the most optimal location
Primary
Secondary
(2) Authoritative DNS server responds with list of IPs
(3) L7 switch access DNS servers and responses and determines the most optimal site, moving that IP to the top of the list
Layer-7 Load Balancing Switch
Layer-7 Load Balancing Switch
Primary Authoritative DNS
Layer-7 HealthChecks
Secondary Authoritative DNS
inContact Cluster
InContact Cluster

Figure 10 - NICE inContact Redundant ACD model

Redundant SQL Servers and IIS Servers with Load Balancing include the following:

This document includes proprietary information of NICE inContact, Inc. This document is for information purposes only and is subject to change without notice. The information contained in this document represents the current view of NICE inContact, Inc., on the issues discussed as of the date published and does not constitute legal advice, representation, warranty or guarantee regarding the products or services described or anyone's ability to comply with applicable regulatory requirements.

- Redundant SQL databases utilize real-time two way replication to ensure data integrity and continuity of services. NICE inContact's ACD application can switch active databases with no loss of ACD services.
- Application alerting tools used by the NOC monitor ACD system performance.
- Management tools allow NICE inContact personnel to gracefully transit and move users and contacts from one set of hardware to the next providing for graceful maintenance of the system.
- Client side applications detect network interruptions and automatically reconnect to the platform.
- ACD services are distributed across geographically diverse data center pairs for redundancy and fault tolerance.
- Each data center has the necessary capacity and services to be able to provide voice, data and ACD services.
- As part of our disaster recovery testing, our ACD platform services are tested periodically to validate the ability for ACD to function independently from each data center pair half, ensuring the ability for ACD to be failed to either for the data center pairs, Los Angeles or Dallas, Frankfurt or Munich, Sydney or Melbourne, in the event of an outage at one of the data centers. CXone architecture also locates service in Amazon West (Zone A and B), Amazon East (Zone A and B) and Amazon AU (Zones A and B)

# Security and Compliance

- NICE inContact annually produces a SOC 2 Type 2 report.

- NICE inContact annually produces a PCI DSS Attestation of Compliance suited to cluster.
- NICE inContact was acquired by NICE Systems, LTD in 2016, (but remains a public corporation) and is 404 SOX certified and PCI service level 2 compliant.
- NICE inContact utilizes AWS S3 storage. AWS has such security assertions as ISO 27001, SOC 1, 2, and PCI AOC. These must be requested directly from Amazon. NICE inContact cannot redistribute these assertions.
- NICE inContact collects and rates security profiles of its vendors.
- NICE inContact utilizes Tenable, a PCI Approved Scanning Vendor (ASV), as a 3rd party scanner contracted to perform and qualify quarterly PCI vulnerability scans. Qualys is used for certain Web Application scans.

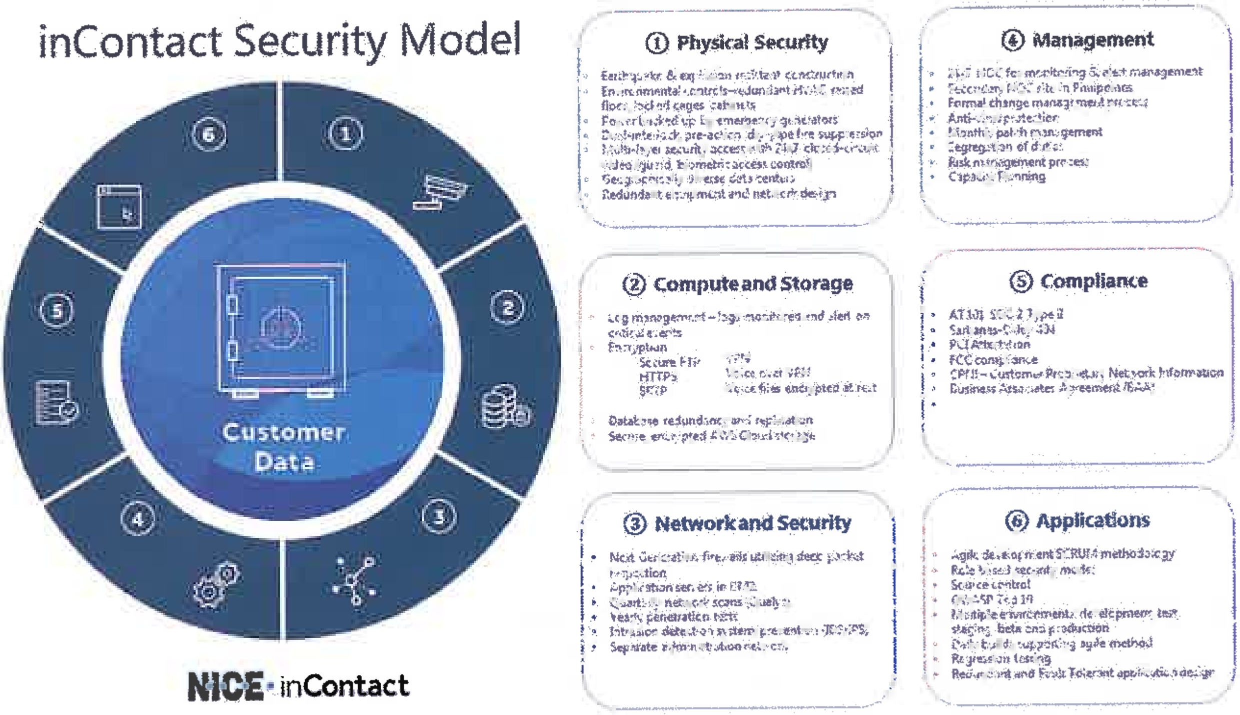
This document includes proprietary information of NICE inContact, Inc. This document is for information purposes only and is subject to change without notice. The information contained in this document represents the current view of NICE inContact, Inc., on the issues discussed as of the date published and does not constitute legal advice, representation, warranty or guarantee regarding the products or services described or anyone's ability to comply with applicable regulatory requirements.

- NICE inContact utilizes Tenable, to do web application scans internal to the organization
- NICE inContact conducts at least yearly 3rd party penetration testing.
- NICE inContact requires yearly CPNI and Security Training for each employee.
- Many industries have their own specific compliance and regulatory requirements. NICE inContact provides tools that enable secure data base and computer telephony integrations (CTI) that enable customers to build compliant applications.
- Executed model contracts can allow NICE inContact to act as a Data Processor in the European Union Market.
- NICE inContact complies with requirements GDPR
- NICE inContact has a dedicated security officer group, the Trust Office, that reports to the Chief Security Officer and works in conjunction with NICE inContact's Internal Audit department, which has security assessment and regulatory compliance as well as audit responsibilities.

## NICE inContact Layers of Security

Numerous controls within the NICE inContact network infrastructure focus on security at all levels of the company. A diagram of the NICE inContact Layers of Security on its Dallas, Los Angeles, Frankfurt, Munich, Melbourne, and Sydney platforms provides a summary of those controls.

This document includes proprietary information of NICE inContact, Inc. This document is for information purposes only and is subject to change without notice. The information contained in this document represents the current view of NICE inContact, Inc., on the issues discussed as of the date published and does not constitute legal advice, representation, warranty or guarantee regarding the products or services described or anyone's ability to comply with applicable regulatory requirements.



## inContact Security Model

**① Physical Security**

- Earthquake & explosion resistant construction
- Environmental controls–redundant HVAC raised floor, locked cages, cabinets
- Power backed up by emergency generators
- Dual-interlock, pre-action, dry-pipe fire suppression
- Multi-layer security, access with 24x7 closed-circuit video, guard, biometric access control
- Geographically diverse data centers
- Redundant equipment and network design

**④ Management**

- 24x7 NOC for monitoring & alert management
- Secondary NOC site in Philippines
- Formal change management process
- Anti-virus protection
- Monthly patch management
- Segregation of duties
- Risk management process
- Capacity Planning

**② Compute and Storage**

- Log management – logs monitored and alert on critical events
- Encryption

  Secure FTP VPN
  HTTPs Voice over VPN
  SFTP Voice files encrypted at rest

- Database redundancy and replication
- Secure encrypted AWS Cloud storage

**⑤ Compliance**

- AT101 SOC 2 Type II
- Sarbanes-Oxley 404
- PCI Attestation
- FCC compliance
- CPNI – Customer Proprietary Network Information
- Business Associates Agreement (BAA)
-

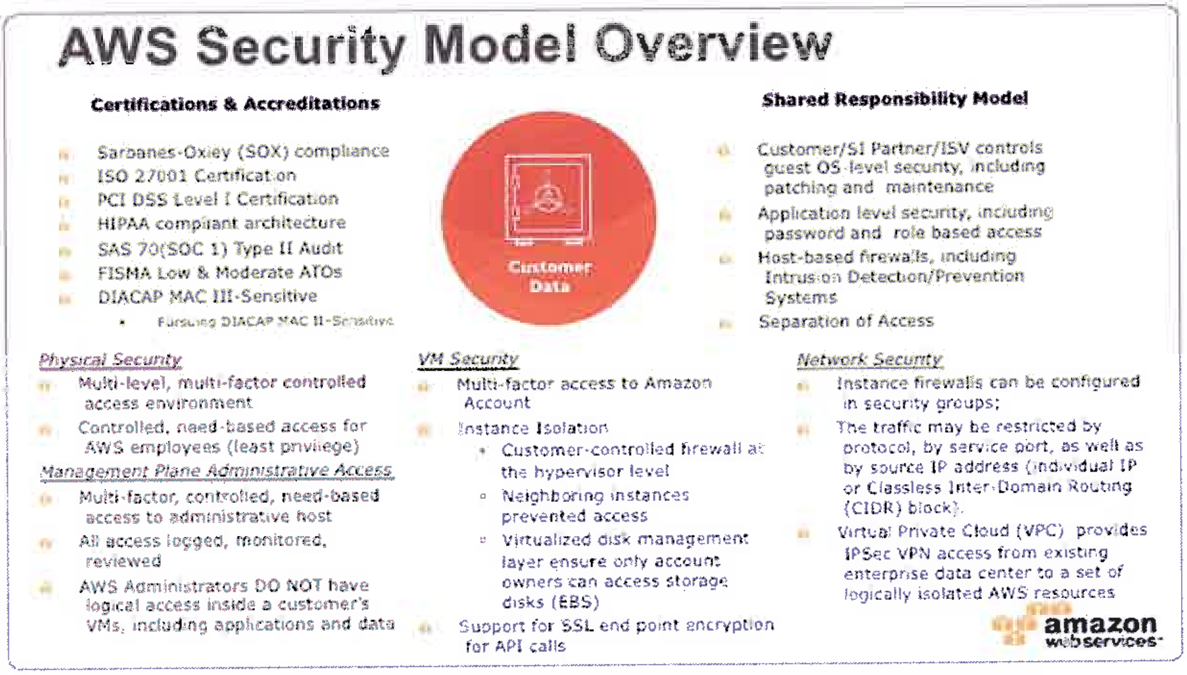
**③ Network and Security**

- Next Generation firewalls utilizing deep packet inspection
- Application servers in DMZ
- Quarterly network scans (Qualys)
- Yearly penetration tests
- Intrusion detection system/prevention (IDS/IPS)
- Separate administration network

**⑥ Applications**

- Agile development SCRUM methodology
- Role based security model
- Source control
- OWASP Top 10
- Multiple environments: development, test, staging, beta and production
- Daily builds supporting agile method
- Regression testing
- Redundant and Fault Tolerant application design

**Figure 11 – NICE inContact "classic" Layers of Security as Defense-in-Depth**



## AWS Security Model Overview

**Certifications & Accreditations**

- Sarbanes-Oxley (SOX) compliance
- ISO 27001 Certification
- PCI DSS Level I Certification
- HIPAA compliant architecture
- SAS 70(SOC 1) Type II Audit
- FISMA Low & Moderate ATOs
- DIACAP MAC III-Sensitive
  - Pursuing DIACAP MAC II-Sensitive

**Shared Responsibility Model**

- Customer/SI Partner/ISV controls guest OS-level security, including patching and maintenance
- Application level security, including password and role based access
- Host-based firewalls, including Intrusion Detection/Prevention Systems
- Separation of Access

*Physical Security*

- Multi-level, multi-factor controlled access environment
- Controlled, need-based access for AWS employees (least privilege)

*Management Plane Administrative Access*

- Multi-factor, controlled, need-based access to administrative host
- All access logged, monitored, reviewed
- AWS Administrators DO NOT have logical access inside a customer's VMs, including applications and data

*VM Security*

- Multi-factor access to Amazon Account
- Instance Isolation
  - Customer-controlled firewall at the hypervisor level
  - Neighboring instances prevented access
  - Virtualized disk management layer ensure only account owners can access storage disks (EBS)
- Support for SSL end point encryption for API calls

*Network Security*

- Instance firewalls can be configured in security groups;
- The traffic may be restricted by protocol, by service port, as well as by source IP address (individual IP or Classless Inter-Domain Routing (CIDR) block).
- Virtual Private Cloud (VPC) provides IPSec VPN access from existing enterprise data center to a set of logically isolated AWS resources

**Figure 12 – NICE inContact AWS Layers of Security as Defense-in-Depth**

This document includes proprietary information of NICE inContact, Inc. This document is for information purposes only and is subject to change without notice. The information contained in this document represents the current view of NICE inContact, Inc., on the issues discussed as of the date published and does not constitute legal advice, representation, warranty or guarantee regarding the products or services described or anyone's ability to comply with applicable regulatory requirements.

# Security and Network Design

- NICE inContact utilizes segmented networks, protecting customer facing applications with secure DMZs, or, in the case of AWS, security groups and rules.
- Production voice services are segmented in to a separate internal production network.
- NICE inContact's production, lab and corporate networks are separated from each other physically, logically and by security permissions.
- Virus and Malware protection software is installed on all corporate, lab and production servers, desktops. Amazon maintains VPCs, virtual networks and subnet with security groups and ACLs.
- Regular, timely patch management is performed.
- A fully managed Intrusion Detection System and Intrusion Prevention System, IDS/IPS, is continuously monitoring NICE inContact's threat surface.

# Security and Data Transport

- 
- Customer data can be sent using SFTP to encrypt transmitted data and can be encrypted while at rest on the EFT/SFTP server.
- SFTP data storage utilizes encryption, a DMZ gateway, and a separate internal network to house the EFT/SFTP server in order to assure PCI compliance for stored sensitive data.

This document includes proprietary information of NICE inContact, Inc. This document is for information purposes only and is subject to change without notice. The information contained in this document represents the current view of NICE inContact, Inc., on the issues discussed as of the date published and does not constitute legal advice, representation, warranty or guarantee regarding the products or services described or anyone's ability to comply with applicable regulatory requirements.

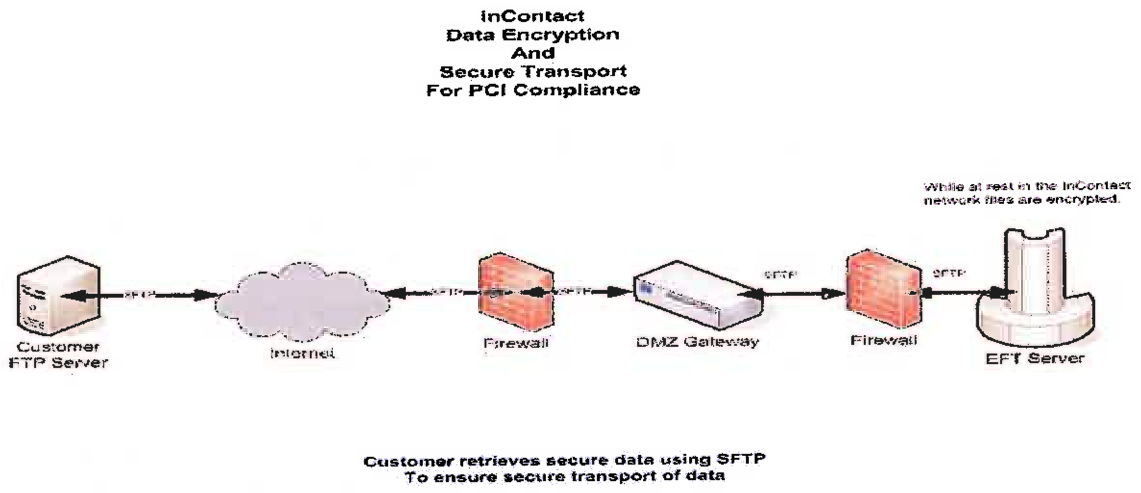


**Figure 13 - NICE inContact Secure Data Transport**

# Security and Client Side Connections

- NICE inContact provides MAX (My Agent Experience), a client browser application that is a modern multi-channel thin client agent desktop for handling voice, email, chat, voicemail, SMS, work items, and social media
- Client side applications use encryption to protect customer data. Client browser applications utilize HTTPS/Port 443 to secure essential browser communications.[
- NICE inContact offers VPN and MPLS connections to secure specific data services such as VoIP.]
- Web services require unique Business Unit and user credentials.

This document includes proprietary information of NICE inContact, Inc. This document is for information purposes only and is subject to change without notice. The information contained in this document represents the current view of NICE inContact, Inc., on the issues discussed as of the date published and does not constitute legal advice, representation, warranty or guarantee regarding the products or services described or anyone's ability to comply with applicable regulatory requirements.

# Security and Platform Users

- The NICE inContact ACD platform uses a multi-tenant architecture. ACD customers do not have their own unique virtual machines or virtual database nor do they have customer specific discrete executables that are running on the ACD servers. Logical isolation of data and services is controlled by the ACD application which uses a unique Business Unit (BU) ID for each customer to logically separate BU data and control BU services. Within each customers BU, data access is controlled using a role-based access password security model. Allowing each customer access to only their BU's data and within that BU, individual users can have different levels of access.
- Passwords can be designed to utilize strong password protection, requiring specific numbers of alpha and numeric characters, life spans, attempt failure limitations and email notifications upon change.

# Security and Internal Policies

- All new employees undergo drug and background checks.
- NICE inContact employs separation of duties to limit access to critical systems, programs and data to the appropriate users and job descriptions.
- NICE inContact secures its corporate facilities with a card-controlled access system and requires all visitors to be badged and accompanied while at the offices.
- All employees receive security awareness and policy training.
- NICE inContact has documented computer and network security policies and processes (see below in "References" which link to NICE inContact Privacy Policy and NICE Privacy Shield Certification; NICE inContact has multiple other governing policies as well, but these mentioned are made public on NICE inContact.com) that govern all corporate users. Standard operating procedures are documented to memorialize key company processes, made required reading for employees and based on Job descriptions.
- Regular external and internal audits are performed.
- Operations maintains and follows a documented POP site work policy.

This document includes proprietary information of NICE inContact, Inc. This document is for information purposes only and is subject to change without notice. The information contained in this document represents the current view of NICE inContact, Inc., on the issues discussed as of the date published and does not constitute legal advice, representation, warranty or guarantee regarding the products or services described or anyone's ability to comply with applicable regulatory requirements.

# Network Operations Center (NOC)

- 7x24x365 staffing. As customer design determines, this staffing may include support in the Philippines, which maintains NOC, technical support, database, and systems administration operational staff.
- Automated monitoring and alerting tools for hardware, applications, environmental controls and network events
- Automated testing of system components
- Defined and documented controls and procedures for managing the network and network events
- All events are tracked in a trouble ticketing system and tickets are tracked to determine adherence to internal and external SLAs

**Figure 14 - NICE inContact 24 x 7 x 365 NOC**

# Change Management:

- NICE inContact uses a documented Change Management Process that includes named members of a change advisory board (CAB) comprised of stake holders from engineering, operations and customer services teams.
- NICE inContact maintains a Technical Risk Review Board (TRRB) to assess all technical changes that impact production for technical level risk and impact. This risk review meets prior to the CAB to expose changes to peer scrutiny before promoting a change to the change advisory board.

This document includes proprietary information of NICE inContact, Inc. This document is for information purposes only and is subject to change without notice. The information contained in this document represents the current view of NICE inContact, Inc., on the issues discussed as of the date published and does not constitute legal advice, representation, warranty or guarantee regarding the products or services described or anyone's ability to comply with applicable regulatory requirements.

- All production changes require the creation of a Change Control Request (CCR) which must be reviewed and approved by the first the TRRB then CAB before the change can be implemented.
- NICE inContact maintains a practice that allows for an Emergency Change Control Board (ECCB) to meet when circumstances require. Such practice could enable appropriate assessment of risk and impact during a disruption of services.
- NICE inContact uses a defined maintenance window along with maintenance notifications to its customers.
- All changes are developed and tested in multiple environments prior to production release. Those environments include Lab, Staging and Beta before final release to Production.
- NICE inContact provides a Trust Site for customers to view system health and obtain information about events and notifications.

# Security and Patching Process

## Windows Systems

- If proof-of-concept code is publicly available regarding a possible exploit, or if a new critical security patch is released, NICE inContact is required to apply patches to affected NICE inContact systems as soon as possible to immediately remediate the vulnerability to the customer's hosted environment.
- Microsoft Critical Updates are applied on a regular schedule, typically a 30-day patch cycle beginning with Microsoft's Patch Tuesday.
- Patches considered critical should not wait for next month's patching.
- Patches and upgrades are documented in a Change Control Record and reviewed by NICE inContact's Change Management Board for impact/risk analysis and necessary actions taken before subsequent approval.
- Patches and upgrades are first tested in our lab, then alpha and beta clusters, then finally into production.
- The NICE inContact operations teams update or patch all applicable NICE inContact devices.
- Patching takes place during a set maintenance window (normally covering 3 hours). Such maintenance can result in a brief interruption of services, but customers are notified if a potential interruption might occur while servers are rebooted or clusters are failed over.

## Non-Windows Systems & Software

Linux and other non-Windows operating systems and devices are patched on an ad-hoc basis, but follow the same Change Control Board process and cycle as above. Current versions are known and compared to relevant CVEs (common vulnerabilities and exposures) then remediated.

Non-windows, or third-party software is evaluated by Trust, using Security Center and other reports, and vulnerabilities are communicated to respective owners and groups, i.e. SysOps. Critical and high vulnerabilities should be patched within 90-days.

## Tools

Automated scanning of the Windows environment is done through an internal tool called 'infra-tools'. This tool is run by SysOps and ensures machines that are not patched are flagged and followed up on for remediation.

## Service Level Objectives

The service level objectives for applying patches ensures that known vulnerabilities are remediated in a timely manner and are compliant with PCI-DSS requirements. A scale of critical, high, medium, and low is used to describe patch risk.

Critical: 30-days

High: Within 60-days

Medium: Within 90 days

Low: *At discretion of device owner group. Trust communicates vulnerabilities via Security Center and other reports.

## Exceptions

For servers and devices that are not communicating with the WSUS servers and able to pull updates, manual remediation and cataloguing is performed. Reports of unpatched servers are provided to Trust for visibility and tracking monthly.

# Vendor Security Review Process

When internal NICE inContact departments requires a new vendor to be considered to supply a NICE inContact product or service, a vendor assessment and approval review process is initiated in order to provide a security profile of the vendor. A vendor dossier is created. Trust and/or Internal Audit performs a review of the vendor. Critical vendors receive other reviews on the one-year anniversary of acceptance. Upon completion of reviews, the vendor dossier generally contains the following vendor artifacts:

- Vendor Security Questionnaire (VSQ)
- Corrective Action Plan (CAP)
- NICE inContact Vendor Security Exhibit (Addendum)
- Other vendor submission collateral such as SOC 2, PCI AOC, Business Associates Agreement (BAA), and or ISO certifications
- Vendor Security Questionnaire with vendor security profile questions answered

This dossier reflects both the initial vendor security review and the anniversary vendor review collateral.

NICE inContact maintains a process flow for performing this vendor security review process.

# Disaster Recovery/Resiliency

To provide Disaster Recovery confidence, NICE inContact maintains a Resiliency Event Management program that begins with design.

- NICE inContact networks are designed with high capacity, fault tolerant equipment, utilizing multiple service providers.
- Tested fail-over automation in the design of data networks, telecom networks, computer networks and applications.
- Additionally, walk through and fail-over drills of background operational processes and components are conducted periodically.
- NICE inContact maintains a 7x24x365 NOC with additional on call staffing for other critical functions.
- NICE inContact data centers are housed in carrier grade facilities (see data centers, p. 6).
- Mission critical data is replicated or backed up as determined by data requirements.
- Backed-up data is stored or replicated to data center locations in diverse geographical areas to ensure survivability in the event of a data center disaster.
- As mentioned in the "NICE inContact ACD Application Design" section above, our USA and European services are tested periodically to validate the ability for ACD to function independently from each data center. This testing, as part of regular maintenance and patching activities, routes all contact processing from one data center to the other, effectively validating the ability for those systems to function independently.

This document includes proprietary information of NICE inContact, Inc. This document is for information purposes only and is subject to change without notice. The information contained in this document represents the current view of NICE inContact, Inc., on the issues discussed as of the date published and does not constitute legal advice, representation, warranty or guarantee regarding the products or services described or anyone's ability to comply with applicable regulatory requirements.

- NICE inContact maintains a documented Resiliency Event Management (Disaster Recovery) Plan that defines the contacts, escalations, and documents the controls necessary to manage outages and service disasters.

This document includes proprietary information of NICE inContact, Inc. This document is for information purposes only and is subject to change without notice. The information contained in this document represents the current view of NICE inContact, Inc., on the issues discussed as of the date published and does not constitute legal advice, representation, warranty or guarantee regarding the products or services described or anyone's ability to comply with applicable regulatory requirements.

# Business Continuity

- Corporate strategies require the NOC and other support teams to be able to work from home or other locations in the event that the corporate offices cannot be used. Formal drills are conducted annually to test the ability to maintain essential operations off-site/at home. Designated staff members as directed by management operate from home for system upgrade and other maintenance activities.
- NICE inContact's Resiliency Event Management (Disaster Recovery) Plan defines a Business Continuity Team to coordinate resources and actions necessary to ensure corporate operational continuity in the event of a disaster.

# Reference Index

- Coresite (LA2) Alameda Facilities (Coresite) – http://www.coresite.com/data-centers/los-angeles/la2 (pg. **Error! Bookmark not defined.**)
- Level 3 colocations - http://www.level3.com/en/resource-library/wp-high-density-data-centers/ (p 7)
- Equinix colocations - **http://www.equinix.com/en_US/platform-equinix/platform-**advantages/ibx-data-centers/ (pg. 9)
- NICE inContact Privacy Policy - http://www.NICE inContact.com/privacy-policy (pg. 27)
- NICE inContact Security in the Cloud - http://www.NICE inContact.com/call-center-solution-finder/learn-about-security-cloud (pg. 5)
- NICE inContact Security and Compliance - http://www.NICE inContact.com/sites/default/files/resources/ds-call-center-pci-compliance.pdf (pg. 22)
- NICE inContact Network - http://www.NICE inContact.com/call-center-software/network-connectivity (pg. 25)
- Safe Harbor (Department Of Commerce after EU Court Decision) – http://export.gov/safeharbor/
- NICE Systems Privacy Shield https://www.privacyshield.gov/participant?id=a2zt0000000TP4hAAG
- Class 4 Switch - http://en.wikipedia.org/wiki/Class_4_telephone_switch#Sector_and_access_tandems (pg. **Error! Bookmark not defined.)**
- Role-based Access - http://en.wikipedia.org/wiki/Role-based_access_control (pg. 27)
- SS7 Call Control - http://en.wikipedia.org/wiki/Signaling_System_7 (pg. 11)
- RESPORG - http://en.wikipedia.org/wiki/RespOrg (pg. 12)

This document includes proprietary information of NICE inContact, Inc. This document is for information purposes only and is subject to change without notice. The information contained in this document represents the current view of NICE inContact, Inc., on the issues discussed as of the date published and does not constitute legal advice, representation, warranty or guarantee regarding the products or services described or anyone's ability to comply with applicable regulatory requirements.

- Approved Scanning vendors - https://www.pcisecuritystandards.org/pdfs/asv_report.html (pg. 22)
- What is SIP? - http://en.wikipedia.org/wiki/Session_initiation_protocol (pg. 11, 20)
- What is CPNI - http://en.wikipedia.org/wiki/Customer_proprietary_network_information (pg. 23)
- Blade Chassis Architecture - http://en.wikipedia.org/wiki/Blade_server (pg. 20)
- HP Carrier Grade Hardware - http://www.hp.com/products1/servers/carrier_grade/index.html?jumpid=reg_R1002_USEN (pg. 20)
- European Telecommunications Standards Institute (ETSI) - http://www.etsi.org/index.php (pg. 20)
- Layer 7 switching - http://en.wikipedia.org/wiki/Layer_7_switch (multi-layer) (pg. 20)
- Team Foundation Server - http://en.wikipedia.org/wiki/Team_Foundation_Server (pg. 4)
- Cloud Security Alliance – CSA https://cloudsecurityalliance.org/ (pp. **Error! Bookmark not defined., Error! Bookmark not defined.**)

# Glossary and Acronyms

**BGP** – Border Gateway Protocol, a routing protocol used to span autonomous systems on the internet. BGP exchanges routing information between networks.

**CCTV** – Closed Circuit Television

**ETSI** – The European Telecommunications Standards Institute, is officially responsible for standardization of Information and Communication Technologies (ICT) within Europe

**DMZ** – is a physical or logical subnetwork that contains and exposes an organization's external services to a larger untrusted network, usually the internet

**DS3** – A high capacity digital facility capable of processing up to simultaneous 672 calls or 44.736 mbps of data.

**GigE** – Gigabit Ethernet interfaces capable of processing 1,000,000,000 bits/s

**10 Gig** – 10 Gigabit Ethernet interfaces capable of processing 10,000,000,000 bits/s

**HP** – Hewlett-Packard is one of the world's largest information technology companies operating in nearly every country

**HTTP/HTTPS** – Hyperext Transport Protocol and Hyperext Transport Protocol Secure – a networking protocol used extensively for Web traffic.

This document includes proprietary information of NICE inContact, Inc. This document is for information purposes only and is subject to change without notice. The information contained in this document represents the current view of NICE inContact, Inc., on the issues discussed as of the date published and does not constitute legal advice, representation, warranty or guarantee regarding the products or services described or anyone's ability to comply with applicable regulatory requirements.

**ISP** – Internet Service Provider, a nationwide provider of internet services.

**Layer 3** -- The third layer of the seven-layer OSI model of computer network and is responsible for routing packets.

**Layer 7** -- The seventh layer of the seven-layer OSI model of computer network. Layer 7 devices allow packet inspection at the application layer for better security.

**MPLS** – Multi Protocol Label Switching is a mechanism in high-performance data networks that directs data from one network node to the next based on short path labels.

**NAS** - Network-Attached Storage is a file-level computer data storage connected to a computer network to provide data storage and access to computers on that network.

**NEBS** – Network Equipment Building System which describes a system to standardize equipment that would be installed in a central office.

**PCI DSS** – Payment Card Industry Digital Security Standards is a worldwide security standard created to help payment card industry organizations prevent credit card fraud.

**POP** – Point of Presence or data center.

**RESPORG** – Responsible Organization is a term that refers to companies that have access to the database or Service Management System (SMS) that controls the routing of all toll free numbers.

**RTP** – Real Time Transport Protocol, a standardized packet format for delivering audio and video over IP networks

**Safe Harbor** – A framework developed by the U.S. Department of Commerce to bridge the different privacy approaches of the U.S.A. and the European Union. It is currently deprecated in the EU by a European court ruling, but NICE inContact still abides by it.

**Privacy Shield** – The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks were designed by the U.S. Department of Commerce, and the European Commission and Swiss Administration, respectively, to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce.

The Privacy Shield program, which is administered by the International Trade Administration (ITA) within the U.S. Department of Commerce, enables U.S.-based organizations to join one or both of the Privacy Shield Frameworks in order to benefit from the adequacy determinations.

**SAN** -- storage area network is an architecture to attach remote computer data storage devices such as disk arrays to servers

This document includes proprietary information of NICE inContact, Inc. This document is for information purposes only and is subject to change without notice. The information contained in this document represents the current view of NICE inContact, Inc., on the issues discussed as of the date published and does not constitute legal advice, representation, warranty or guarantee regarding the products or services described or anyone's ability to comply with applicable regulatory requirements.

**SBC** – Session Border Controller – a device installed at the edge of a VoIP network that acts as a VoIP firewall, controlling ingress and egress to the VoIP network.

**SIP** – Session Initiated Protocol is a communications protocol commonly used to initiate Voice over IP or VoIP calls.

**SOC 2** – AICPA provides a Service Organization Control (SOC) structure that NICE inContact services qualify for, and supersedes both the SSAE 16 and SAS70.

**SRTP** – Secure Real Time Transport Protocol, is a method to encrypt the audio on VoIP calls

**T1** – A high capacity digital facility capable of processing up to 24 simultaneous calls or 1.536 mbps of data.

**TDM** – Time Division Multiplexing is a method used to multiplex two or more digital or analog signals in to one signal by allocating a specific time slot for each multiplexed signal.

**TF** – Toll Free numbers are a set of numbers using an 8XX NPA format for which the toll charges associated with the call are paid for by the owner of the toll free number.

This document includes proprietary information of NICE inContact, Inc. This document is for information purposes only and is subject to change without notice. The information contained in this document represents the current view of NICE inContact, Inc., on the issues discussed as of the date published and does not constitute legal advice, representation, warranty or guarantee regarding the products or services described or anyone's ability to comply with applicable regulatory requirements.

# Appendix D. Verizon VCE BroadSoft/Cisco Security

BroadSoft BroadCloud applications and services are running on multiple servers within BroadSoft BroadCloud Datacenters.

BroadSoft BroadCloud provides applications and services that are assured by the implementation of security and availability methods and procedures designed to cover physical access and protection, network connectivity, remote and local access, application and server management, availability and customer sensitive data.

## Physical Security

BroadSoft BroadCloud partners with datacenter operators with years of experience in design, implementation, and operation of large-scale datacenters. These facilities provide physical, environmental and access security, protecting BroadSoft BroadCloud's physical and virtual application environments.

### Facility

- 24x7x365 On-site security personnel
- Nondescript and unmarked facilities with natural boundary protection
- Silent alarm system with automatic notification of local law enforcement
- Building code compliance to local governmental standards

### Environmental Safeguards

- Fully redundant HVAC facilities
- Automatic Fire suppression systems, dual alarmed (heat/smoke), dual interlock with cross-linked event management
- N+1 redundant UPS power system supporting entire datacenter capacity, with redundant backup generators
- Where appropriate, localized disaster compliance (seismic, flood control)

### Access

- Biometric scanning and/or 2-factor authentication for access
- All ingress/egress through vestibules (man-traps)
- Access requires valid government issued photo ID, and all access history is recorded for audit purposes
- Authorization required prior to access and is only provided for legitimate business need

- Shipping and receiving are walled off from co-location areas
- For both ingress and egress, all material is inspected upon arrival by on-site security staff.

### Network

External network security falls into two generalized categories: firewall protection and intrusion detection and prevention. When peer connections are allowed to BroadSoft BroadCloud, VPN peering provides secure access.

Additional internal network configuration isolates web, application, and database layers to further eliminate possible intrusion.

### Firewall

- The firewalls are configured in multiple zones for tiered security. All public access to BroadSoft BroadCloud applications and services traverses a demilitarized zone (DMZ) for added security
- The firewalls are configured to only allow traffic specific to BroadSoft BroadCloud applications and services. All other traffic is restricted
- Access policies are defined based on UDP/TCP service port, source IP addresses, and destination IP addresses. Access to a specific application or service is minimized to the smallest possible set of service ports and IP addresses
- FTP and telnet are blocked both at the firewall, and where necessary, at the server OS level, preventing anonymous access

### Intrusion Detection and Prevention

- Both hardware and software solutions identify, classify, and stop malicious traffic before it affects application continuity
- Inline prevention technologies take preventive action on a broad range of threats including Denial of Service (DoS), without the risk of dropping legitimate traffic
- Network protection from policy violations, vulnerability exploitations, and anomalous activity through detailed inspection of traffic in Layers 2 through 7

### VPN

Where needed to connect to service provider networks and enhanced content providers, connection out of the network takes place over IPsec or MPLS VPN. Strong Encryption is used to provide the highest level of peering security.

## Operational and Environmental Security

### User Authentication

Users of BroadSoft BroadCloud applications and services are required to authenticate upon access by means of a valid user ID and password. This and other identifiable information is encrypted by means of SSL (HTTPS) while in transmission from the user's endpoint to/from the BroadSoft BroadCloud application or service.

### Operations Management

- All BroadSoft BroadCloud personnel have background checks performed prior to hire
- Restricted access is only granted to personnel necessary to perform management, maintenance, and monitoring functions
- Customer ticketing is achieved via customer portal, including support history

### Internal Network

- Traffic between public and private networks traverses a proxy server located in a demilitarized zone (DMZ) to improve security in the private network
- Virtual Local Area Networks (VLAN) and firewalls isolate each subnet
- Maintenance access to systems used to deliver services is through an independent IP subnet. Backup connectivity to the management subnet is via out-of-band connectivity to a terminal server using encrypted SSH access, and access to the terminal server is limited to specific BroadSoft IP addresses
- Authentication, authorization, and accounting on network components are controlled down to the command level

### Server Management

- Servers are fully hardened, removing/disabling unnecessary services (SMTP, Telnet, FTP, etc.)
- Operating system and supporting applications are regularly updated to safeguard against emerging vulnerabilities
- User account management manages and limits OS user authorization
- All Command line activity is logged and monitored to prevent unauthorized OS user activity
- Password Control including regular rotation, strong structure, encryption during transmission, and are not stored within BroadSoft BroadCloud environments

### Database

- Database access is controlled and limited to BroadSoft BroadCloud operations resources
- BroadSoft BroadCloud application layers completely segment BroadSoft BroadCloud customer data, thus preventing access by any other customer's data or application
- No external network connectivity allowed on database layer servers
- Password Control including regular rotation, strong structure, and application specific passwords where necessary

### Availability

- Carrier grade hardware utilized throughout the datacenter
- Physical redundancy server configurations for web, application and database server layers
- Servers deployed with redundancy across separate physical hosts and separate physical datacenters
- Redundant connectivity throughout the internal network
- Multiple ISPs connected and homogenized into the BroadSoft BroadCloud datacenter to eliminate single point of connectivity failure
- Highly available storage/disks including redundant power supplies, controllers, RAID 5 arrays with live spares, and network connections
- All datacenter hardware fed by redundant and disparate commercial power, backed up by UPS and generators

### Backups

- Automation provides regularly scheduled backups of DB and server images
- Synchronization technology sends regular updates of backups electronically to offsite and geographically disparate storage
- All local and offsite backups are monitored and automatically retry as needed
- BroadSoft BroadCloud code objects are regularly backed up both locally and offsite
- Backups are tested regularly

### Disaster Recovery

In the event of a service affecting and potentially long term outage of a datacenter due to a natural disaster or other cause beyond the control of BroadSoft BroadCloud, backups can be retrieved from offsite storage, and can rebuild effected applications and services.

### Sensitive Data

BroadSoft BroadCloud recognizes that in some cases, certain user sensitive data may exist within the scope of data managed on behalf of its customers.

In these cases, additional care will be taken to conform to the local governing laws for this data, regardless of region. This may be in the form of managing such data within the confines of the region, or country.

No such sensitive data shall ever be taken out of the BroadSoft BroadCloud datacenters or its established backup networks. Wherever possible, BroadSoft BroadCloud will manage sensitive data under these seven guidelines:

- Notice – End-users will be notified upon collection of end-user sensitive data
- Purpose – The data collected will only be used for the purpose of providing BroadSoft BroadCloud services
- Consent – Sensitive data should not be disclosed without the end-user's consent
- Security – Collected data will be kept safe
- Disclosure – End-users are to be aware of who is collecting sensitive data
- Access – End-user should be able to correct inaccurate data
- Accountability – End-Users should be able to hold BroadSoft BroadCloud accountable for these guidelines

BroadSoft BroadCloud is continually updating its practices and policies regarding datacenter deployment and security, as well as reviewing and from time to time, changing service providers and operators it uses to provide BroadSoft BroadCloud services.

# Appendix E. Cyber Security Program

Please refer to our attached icon(s) below, pertaining to the Cyber Security Program documentation. For hardcopy purposes, please review the following page(s).

Cyber_Risk_Program
s.docx

# Rethink risk with evidence-based security

## Cyber Risk Programs

verizon✓

**Managing risk can feel like a moving target. And although you may not be able to plan for every possibility, you can use historical trends as a guide to help you improve your security posture.**

The Verizon 2017 Data Breach Investigations Report (DBIR) found that 88% of data breaches fit into nine attack patterns, and the patterns impact each industry differently. This information can help you decide where to focus your security efforts.

**88%** of data breaches fit into nine attack patterns[1].

## Objective, evidence-based and collaborative.

Verizon Cyber Risk Programs bring objective, data-driven risk analysis to your risk-management strategy. We have three different service levels available, so we can help you protect your entire organization with a solution that best meets your business needs. Our experts will work with you to understand your risk when compared with the threat scenarios and attack patterns identified in the DBIR. We'll also create a plan that prioritizes your problem areas so you can get the most out of your security budget.

We use a proprietary scoring method to help you prove due diligence to auditors. Important stakeholders and business leaders will have confidence in your security strategy—and you'll have better peace of mind knowing your organization is protected.

**Make more-informed cyber-risk decisions, backed by the integrity, capability and reliability of our services and people.**

## Pinpoint the threats.

When you know where the biggest threats are, you can plan accordingly. Our experts can show you which measures are the most important to protect your business. We can help with:

- Periodic reviews to verify your controls are working and help find potential weaknesses in your security strategy.
- Expert assessments and diagnostic methodologies, built from years of legacy technologies.
- Insights from more than a decade of DBIR data highlighting which threat patterns lead to actual data breaches.
- Direct mappings to the most common cyber-risk management frameworks so you can better understand your level of risk across likely scenarios.

[1] Verizon 2017 Data Breach Investigations Report

## Three levels of protection.

Your threat profile and security needs are specific. Our solution is designed to meet those needs by using industry-specific data to defend against the threats that matter to you most.

## Risk rating.

Evaluate your risk-reducing controls simply and effectively.

- Reviews your external security controls against the most common threats.
- Produces a quarterly diagnostic score.
- Provides additional guidance to help reduce cyber risk, including references to DBIR attack patterns.
- Allows industry/peer benchmarks.

## Risk assessment.

Comprehensive and maturity-based assessment against most cyber threats.

- Reviews your internal and external security controls against a broad number of cyber threats.
- Produces quarterly risk-assessment scores against key security controls.
- Includes risk-reducing recommendations.
- Lets you calculate and compare your controls against key control frameworks and industry peers.

## Risk evaluation.

Customizable activities to examine your risk level, based on your methodology.

- Reviews external, internal, partner and subsidiary security controls.
- Provides a monthly adaptive risk score.
- Lets you select your risk-reducing controls and then examine and rate your posture against key control frameworks and industry peers (depending on scoring methods).
- Based on your maturity and specific risk-scoring methodology.

## Build a strong defense with insight and data.

Cyber Risk Programs help you better defend against threats by managing risk more deliberately, so you can move from:

- Simple intuition to risk models based on evidence. Different industries have different threat profiles, which require different remediation priorities. Our methodology can help you better understand your risk, prioritize remediation efforts and use proactive security measures.
- Subjective risk scoring to evidence-based scoring. We've converted threat intelligence from the DBIR into actual risk analysis so you can better understand and guard against threats.
- A fragmented view to a broader one. Nowadays, security can be fragmented, with many vendors and technologies working independently. We provide visibility across your network, consolidating control of your security products and services to help you respond more effectively to an attack.

## ;'hreat protection with an advantage.

Get better peace of mind with expertise that helps you manage risk.

- Global visibility. Our network provides insights of recent threats and attacks.
- Deep expertise. We investigate some of the most high-profile global breaches each year.
- Security intelligence. We know how the attackers work and what they want.

### Learn more.

To find out how Verizon Cyber Risk Programs can help your business build a better foundation for defense, contact your account manager or visit:

**VerizonEnterprise.com/products/security**

# Appendix F. Evidence of Liability Insurance

Please refer to our attached icon(s) below, pertaining to Evidence of Liability Insurance. For hardcopy purposes, please review the following page(s).

Verizon - EOI 2M CGL-2M AL-1M EL 20:

Verizon 10.31.2017-18 EO.C

ACORD®

# CERTIFICATE OF LIABILITY INSURANCE

DATE(MM/DD/YYYY)
06/19/2018

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

**IMPORTANT:** If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

Holder Identifier :

PRODUCER
Aon Risk Services Northeast, Inc.
New York NY Office
199 Water Street
New York NY 10038-3551 USA

CONTACT NAME:
PHONE (A/C. No. Ext): (866) 283-7122
FAX (A/C. No.): (800) 363-0105
E-MAIL ADDRESS:

INSURED
Verizon Communications Inc.
1095 Avenue of the Americas
New York NY 10036 USA

| INSURER(S) AFFORDING COVERAGE | | NAIC # |
|---|---|---|
| INSURER A: | National Union Fire Ins Co of Pittsburgh | 19445 |
| INSURER B: | New Hampshire Insurance Company | 23841 |
| INSURER C: | American Home Assurance Co. | 19380 |
| INSURER D: | Illinois National Insurance Co | 23817 |
| INSURER E: | | |
| INSURER F: | | |

## COVERAGES

CERTIFICATE NUMBER: 570071819592

REVISION NUMBER:

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

**Limits shown are as requested**

| INSR LTR | TYPE OF INSURANCE | ADDL INSD | SUBR WVD | POLICY NUMBER | POLICY EFF (MM/DD/YYYY) | POLICY EXP (MM/DD/YYYY) | LIMITS | |
|---|---|---|---|---|---|---|---|---|
| A | ☒ COMMERCIAL GENERAL LIABILITY | | | GL4611607 | 06/30/2018 | 06/30/2019 | EACH OCCURRENCE | $2,000,000 |
| | ☐ CLAIMS-MADE ☒ OCCUR | | | | | | DAMAGE TO RENTED PREMISES (Ea occurrence) | $2,000,000 |
| | ☒ Standard Contractual Liability | | | | | | MED EXP (Any one person) | $10,000 |
| | ☒ XCU Coverage is Included | | | | | | PERSONAL & ADV INJURY | $2,000,000 |
| | GEN'L AGGREGATE LIMIT APPLIES PER: | | | | | | GENERAL AGGREGATE | $2,000,000 |
| | ☒ POLICY ☐ PRO-JECT ☐ LOC | | | | | | PRODUCTS - COMP/OP AGG | $2,000,000 |
| | ☐ OTHER: | | | | | | | |
| A | AUTOMOBILE LIABILITY | | | CA 461-15-19<br>AOS | 06/30/2018 | 06/30/2019 | COMBINED SINGLE LIMIT (Ea accident) | $2,000,000 |
| A | ☒ ANY AUTO | | | CA 461-15-20<br>MA | 06/30/2018 | 06/30/2019 | BODILY INJURY ( Per person) | |
| A | ☐ OWNED AUTOS ONLY ☐ SCHEDULED AUTOS | | | CA 461-15-21<br>VA | 06/30/2018 | 06/30/2019 | BODILY INJURY (Per accident) | |
| A | ☐ HIRED AUTOS ONLY ☐ NON-OWNED AUTOS ONLY | | | See Next Page | 06/30/2018 | 06/30/2019 | PROPERTY DAMAGE (Per accident) | |
| | ☐ UMBRELLA LIAB ☐ OCCUR | | | | | | EACH OCCURRENCE | |
| | ☐ EXCESS LIAB ☐ CLAIMS-MADE | | | | | | AGGREGATE | |
| | DED ☐ RETENTION | | | | | | | |
| B | WORKERS COMPENSATION AND EMPLOYERS' LIABILITY Y/N | | | WC014590551<br>AOS | 06/30/2018 | 06/30/2019 | ☒ PER STATUTE ☐ OTH-ER | |
| C | ANY PROPRIETOR / PARTNER / EXECUTIVE OFFICER/MEMBER EXCLUDED? N | N/A | | WC014590550<br>CA | 06/30/2018 | 06/30/2019 | E.L. EACH ACCIDENT | $1,000,000 |
| | (Mandatory in NH) | | | | | | E.L. DISEASE-EA EMPLOYEE | $1,000,000 |
| | If yes, describe under DESCRIPTION OF OPERATIONS below | | | | | | E.L. DISEASE-POLICY LIMIT | $1,000,000 |
| | | | | | | | | |

Certificate No : 570071819592

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)
Evidence of Insurance.

## CERTIFICATE HOLDER

Verizon Communications Inc.
1095 Avenue of the Americas
New York NY 10036 USA

## CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

Aon Risk Services Northeast, Inc.

AGENCY CUSTOMER ID: 570000027366
LOC #:

# ADDITIONAL REMARKS SCHEDULE

Page _ of _

| | |
|---|---|
| AGENCY<br>Aon Risk Services Northeast, Inc. | NAMED INSURED<br>Verizon Communications Inc. |
| POLICY NUMBER<br>See Certificate Number: 570071819592 | |
| CARRIER<br>See Certificate Number: 570071819592 \| NAIC CODE | EFFECTIVE DATE: |

ADDITIONAL REMARKS

THIS ADDITIONAL REMARKS FORM IS A SCHEDULE TO ACORD FORM,
FORM NUMBER: ACORD 25 FORM TITLE: Certificate of Liability Insurance

| INSURER(S) AFFORDING COVERAGE | NAIC # |
|---|---|
| INSURER | |
| INSURER | |
| INSURER | |
| INSURER | |

**ADDITIONAL POLICIES** If a policy below does not include limit information, refer to the corresponding policy on the ACORD certificate form for policy limits.

| INSR LTR | TYPE OF INSURANCE | ADDL INSD | SUBR WVD | POLICY NUMBER | POLICY EFFECTIVE DATE (MM/DD/YYYY) | POLICY EXPIRATION DATE (MM/DD/YYYY) | LIMITS | |
|---|---|---|---|---|---|---|---|---|
| | AUTOMOBILE LIABILITY | | | | | | | |
| A | | | | CA 774-22-65<br>NH - Primary | 06/30/2018 | 06/30/2019 | | |
| A | | | | CA 774-22-66<br>NH - Excess | 06/30/2018 | 06/30/2019 | | |
| | WORKERS COMPENSATION | | | | | | | |
| D | | N/A | | WC014590552<br>FL | 06/30/2018 | 06/30/2019 | | |
| B | | N/A | | WC014590553<br>ME | 06/30/2018 | 06/30/2019 | | |
| B | | N/A | | WC014590549<br>NJ,NY,TX,VA | 06/30/2018 | 06/30/2019 | | |
| B | | N/A | | WC014590554<br>MA,ND,OH,WA,WI,WY | 06/30/2018 | 06/30/2019 | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

ACORD®

# CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)
10/27/2017

**THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.**

**IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).**

| | |
|---|---|
| PRODUCER<br>Beecher Carlson - New York<br>1500 Broadway<br>21st Floor<br>New York NY 10036 | CONTACT NAME: Robert O'Shea, Jr<br>PHONE (A/C, No, Ext): (646)358-8513 FAX (A/C, No): (770) 870-3055<br>E-MAIL ADDRESS: roshea@beechercarlson.com |
| | INSURER(S) AFFORDING COVERAGE — NAIC # |
| | INSURER A : ACE American Insurance Company — 22667 |
| INSURED<br>Verizon Communications Inc.<br>1095 Avenue of the Americas<br>8th Floor<br>New York NY 10036 | INSURER B : |
| | INSURER C : |
| | INSURER D : |
| | INSURER E : |
| | INSURER F : |

## COVERAGES

CERTIFICATE NUMBER: CL17102752425 REVISION NUMBER:

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

| INSR LTR | TYPE OF INSURANCE | ADDL INSD | SUBR WVD | POLICY NUMBER | POLICY EFF (MM/DD/YYYY) | POLICY EXP (MM/DD/YYYY) | LIMITS | |
|---|---|---|---|---|---|---|---|---|
| | □ COMMERCIAL GENERAL LIABILITY<br>□ □ CLAIMS-MADE □ OCCUR<br>□<br>□<br>GEN'L AGGREGATE LIMIT APPLIES PER:<br>□ POLICY □ PRO-JECT □ LOC<br>□ OTHER: | | | | | | EACH OCCURRENCE<br>DAMAGE TO RENTED PREMISES (Ea occurrence)<br>MED EXP (Any one person)<br>PERSONAL & ADV INJURY<br>GENERAL AGGREGATE<br>PRODUCTS - COMP/OP AGG | $<br>$<br>$<br>$<br>$<br>$<br>$ |
| | AUTOMOBILE LIABILITY<br>□ ANY AUTO<br>□ ALL OWNED AUTOS □ SCHEDULED AUTOS<br>□ HIRED AUTOS □ NON-OWNED AUTOS<br>□ □ | | | | | | COMBINED SINGLE LIMIT (Ea accident)<br>BODILY INJURY (Per person)<br>BODILY INJURY (Per accident)<br>PROPERTY DAMAGE (Per accident) | $<br>$<br>$<br>$<br>$ |
| | □ UMBRELLA LIAB □ OCCUR<br>□ EXCESS LIAB □ CLAIMS-MADE<br>□ DED □ RETENTION $ | | | | | | EACH OCCURRENCE<br>AGGREGATE | $<br>$<br>$ |
| | WORKERS COMPENSATION AND EMPLOYERS' LIABILITY Y/N<br>ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? □<br>(Mandatory in NH)<br>If yes, describe under DESCRIPTION OF OPERATIONS below | N/A | | | | | □ PER STATUTE □ OTH-ER<br>E.L. EACH ACCIDENT<br>E.L. DISEASE - EA EMPLOYEE<br>E.L. DISEASE - POLICY LIMIT | <br>$<br>$<br>$ |
| A | Professional Liability/E&O and Cyber Liability | | | EON G21684077 012 | 10/31/2017 | 10/31/2018 | Per Claim<br>Annual Aggregate | $1,000,000<br>$1,000,000 |

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

| CERTIFICATE HOLDER | CANCELLATION |
|---|---|
| Evidence of Insurance | SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS. |
| | AUTHORIZED REPRESENTATIVE<br>R O'Shea, Jr/BMOOR |

# Appendix G. Sample Project Plan

Please refer to our attached icon(s) below, pertaining to the Sample Project Plan. For hardcopy purposes, please review the following page(s).

Sample Project Plan.doc

## Sample Draft

For

# State of West Virginia Preliminary UCCaaS Migration and Transformation Plan

Version 1.0

# Table of Contents

# CHANGE HISTORY

| Revision/Change | Date of Rev/Change | Remarks |
|---|---|---|
| Created v1.0 | November 2018 | First Draft |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

# 1 Document Purpose

The purpose of this Preliminary Transition Plan is to provide an outline of requirements, processes, procedures, and estimated timeframes for the transition of Verizon and UCCaaS and MIPPBX. This Preliminary Transition Plan documents the mutual agreements between State of West Virginia and Verizon, as well as strategies, implementation objectives, and priorities.

# 2 Transition Approach

In support of our transition effort, Verizon will assemble a team of professionals that will be working with State of West Virginia throughout the transition to customize and deliver a plan specific to your needs. At the outset, Verizon will assign a Transition Manager, dedicated to State of West Virginia Transition. The Transition Manager will be the single point of contact to State of West Virginia for all aspects of Governance, communication and escalation during the transition phase.

Verizon has developed over the years a transition methodology that has been used to transition customers into Verizon. This includes a step-by-step, detailed implementation approach and plan that is structured to ensure that our customers will experience a smooth implementation to the new environment. To help avoid transition issues and to mitigate risk, we will work with State of West Virginia to develop an agreed upon transition approach and schedule, detailed in project plans to cover the transition to Verizon.

As outlined below in our Solution framework and transition methodology, our step-by-step approach minimizes risk through:

- Detailed gathering of requirements that are documented in our project definition report and is agreed to in collaboration with State of West Virginia.
- Effective Knowledge Transfer that includes the immersion of Verizon skilled resources into State of West Virginia that begin the process of understanding not only the IT requirements, but also State of West Virginia's business requirements and understanding impacts that may address transition and ongoing support.

### Verizon Transition and Transformation Methodology

Verizon uses five standard methodologies for all new management and support engagements. We avoid a 'Big Bang' approach, but rather an approach that minimize transition risks and enable flawless execution readiness for steady-state support. IT-enabled services and solutions are critical for business revenue generation; operational transitions must be carried out with extreme care in planning and execution. The methodology used by Verizon is based on ITIL and PMI framework and includes:

- **Consulting Approach** - Our approach is consultative, listening to your needs, conducting a gaps analysis, and working with you to develop a customized plan that will mitigate your risk and deliver the outcome in the timeframe and budget that you require.

- **Transition Methodology** - Verizon assembles a team of experts that are familiar with your requirements and works to deliver a successful transition by effectively managing the process and bringing the resources together in a timely manner.
- **Communication Plan** - Development of an effective communication plan where we together establish key stakeholders, identify risk and mitigation plans, reporting requirements, schedule ongoing meetings for project updates and facilitating communication.
- **Transition Change Management** - Tightly managing change via Change Control Process. Integration of standard repeatable processes while providing the flexibility to adapt to change and then execute on these changes.
- **Risk Management** - Verizon brings an experienced team of professionals and proven processes that are integrated into the transition process to enable ongoing management of complex IT environments that require continued secure and compliant environments while undergoing change in a dynamic business arena.
- **Continuous Service Improvement** - Built into each and every transition plan are processes that work toward achieving not only a successful transition, but also one that delivers process improvements that drive efficiencies beginning with transition and continuing throughout steady-state.

# 3 Transition Objectives

Transition is the first and most critical stage of Verizon's phased approach for delivering a next generation networking solution for State of West Virginia. Transition consists of the detailed planning and execution activities required for the successful migration of technical, operational, and managerial responsibilities from the legacy State of West Virginia environment to the Verizon platform. Our solution for State of West Virginia is based on information known to Verizon about the customer environment from the current. Transition consists of the detailed planning and execution activities r environment, as well as from additional information provided by State of West Virginia throughout the RFP process.

Through comprehensive processes and methodologies for transitioning and transforming client networks, Verizon is able to provide a risk-mitigated, converged solution utilizing appropriate subject matter experts (SMEs) and networking professionals. Under the auspices of our Complex Delivery Organization, Verizon designs, engineers, implements, and manages the entire network from end to end. The Verizon approach to transition and transformation is designed to be unobtrusive to the customer, ensuring that the evolution from legacy to next generation networking is done without disruption to State of West Virginia core business operations.

The Verizon Transition Plan is focused on meeting State of West Virginia strategic requirements and achieving service delivery goals. This Transition Plan addresses the continuous processes for moving between service delivery states:

- Implementation and/or transformation of service
- Steady-state operation of service

Verizon assumes that the Transition Period will commence upon the contract effective date and will last approximately 30 months, but subject to planning. This timeline is based upon the dates outlined in the RFP documents. This timeframe is subject to change depending on the date of contract execution and other variables. Verizon is committed to executing the Transition Plan within the prescribed timeframe. Careful communication, planning, and prioritization will also include the State of West Virginia requirements and needs in jointly developing the plan.

## 2.1 Key Objectives

Verizon's key objectives for the successful transition are:

- Development of an agreed Transition Plan and supporting schedules to cover global transition activities, identify roles and responsibilities, costs, timelines, risk and contingency plans and project controls.
- Communication is critical to transition. Verizon believes that the co-ordination between State of West Virginia, State of West Virginia Service Providers and Verizon will require continuous cooperation at all management levels and will ensure that a comprehensive effective communication plan is developed and presented in the first stages of the transition process.
- The Governance structure forms a key part of the long-term integration strategy and assurance of operational compliance with the Agreement and will be created as a priority within the Service Management Organization
- A seamless transition of the existing in-scope services and technical environment with minimal or no disruption to users
- Insure stabilization of the environment.

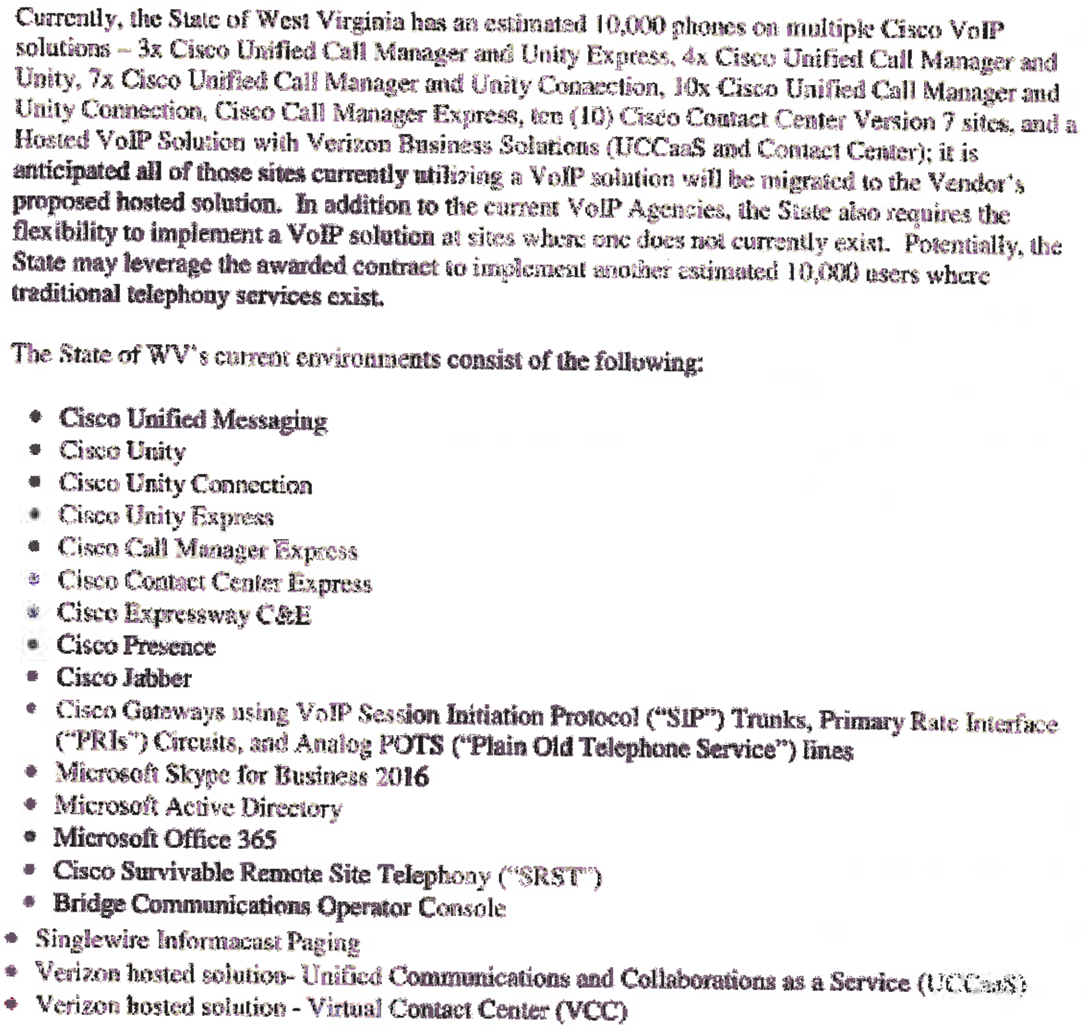
# 3 Transition and Transformation Scope

## 3.1 Project Scope of Work

The final scope of this project will be defined and agreed upon by State of West Virginia and Verizon during the initiating phase. Verizon has agreed to provide State of West Virginia with the products and services listed below based upon the RFP:

- Site Surveys
- Management Takeover (MTO) of legacy Cisco premised-based systems

  **Legacy Cisco**



Currently, the State of West Virginia has an estimated 10,000 phones on multiple Cisco VoIP solutions – 3x Cisco Unified Call Manager and Unity Express, 4x Cisco Unified Call Manager and Unity, 7x Cisco Unified Call Manager and Unity Connection, 10x Cisco Unified Call Manager and Unity Connection, Cisco Call Manager Express, ten (10) Cisco Contact Center Version 7 sites, and a Hosted VoIP Solution with Verizon Business Solutions (UCCaaS and Contact Center); it is anticipated all of those sites currently utilizing a VoIP solution will be migrated to the Vendor's proposed hosted solution. In addition to the current VoIP Agencies, the State also requires the flexibility to implement a VoIP solution at sites where one does not currently exist. Potentially, the State may leverage the awarded contract to implement another estimated 10,000 users where traditional telephony services exist.

The State of WV's current environments consist of the following:

- Cisco Unified Messaging
- Cisco Unity
- Cisco Unity Connection
- Cisco Unity Express
- Cisco Call Manager Express
- Cisco Contact Center Express
- Cisco Expressway C&E
- Cisco Presence
- Cisco Jabber
- Cisco Gateways using VoIP Session Initiation Protocol ("SIP") Trunks, Primary Rate Interface ("PRIs") Circuits, and Analog POTS ("Plain Old Telephone Service") lines
- Microsoft Skype for Business 2016
- Microsoft Active Directory
- Microsoft Office 365
- Cisco Survivable Remote Site Telephony ("SRST")
- Bridge Communications Operator Console
- Singlewire Informacast Paging
- Verizon hosted solution- Unified Communications and Collaborations as a Service (UCCaaS)
- Verizon hosted solution - Virtual Contact Center (VCC)

Transition consists of the detailed planning and execution activities required for the successful migration of technical, operational, and managerial responsibilities from the legacy State of West Virginia environment to the environment supported by Verizon. Our solution for State of West Virginia is based on information known to Verizon about the environment from the current business partnership, as well as from additional information provided by State of West Virginia throughout the due diligence and contracting design and planning sessions.

Verizon proposes to Transition and Transform the following Services:

## Legacy Cisco Managed IPPBX Transition Approach

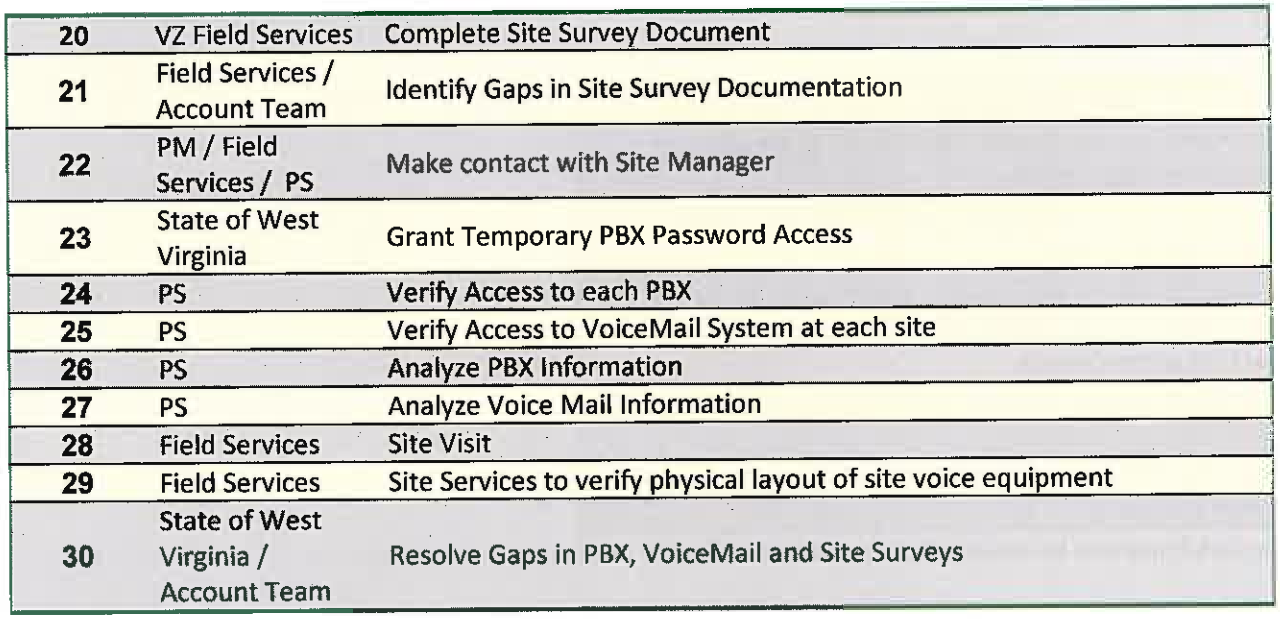
Transition for IP PBX Management will consist of migrating State of West Virginia's IP PBX environment to Verizon. The Transition Plan will not start until all existing Cisco Call Manager clusters, Unity Messaging Systems and Emergency Responder servers are upgraded to the current versions

Key transition actions include:

- State of West Virginia to complete the full upgrade of existing Cisco IPT infrastructure
- Verizon to survey sites and IPT hardware
- Verizon to perform data gathering and compilation of data
- Verizon will assess the design and configuration of all Cisco IPT components
- Determine any remediation requirements
- Perform remediation if required
- Integration Test Plan
- Implementation of Services
- Start-up and Integration Activity
- Stabilization and Management
- Drive increased network availability and efficiency
- Reduce the quantity and severity of network issues
- Provide increased responsiveness for your technical support issues
- Provide access to key technical information
- Provide fast, consistent emergency response to business-critical and outage cases.

## IP PBX Managed Takeover

| 1 | Owner | Staffing |
|---|---|---|
| 2 | State of West Virginia | If any projects are in process, We request that the State Perform the Upgrade of existing IPT infrastructure |
| 3 | VZ PM | Establish SOMI project team and establish weekly meetings with the State of West Virginia Project Team |
| 4 | State of West Virginia / VZ | Finalize Service Levels |
| 5 | VZ | Finalize Additional Evaluation Criteria |
| 6 | Verizon | Establish information exchange process to State of West Virginia ticketing system |
| 7 | VZ | Define & Implement User Help Process |
| 8 | VZ | Obtain Weekly Ticket Summary |
| 9 | PM | Communicate Support Processes to Verizon PMO and State of West Virginia |
| 10 | PM | Provide access information to Verizon Network Operations Center |
| 11 | State of West Virginia | Provide Current Inventory of Voice Network |
| 12 | PS | Provide information for policies and procedures for opening and accessing all trouble tickets |
| 13 | Service Desk | Provide Support Processes for end user assistance |
| 14 | State of West Virginia | Transfer all access information to SE / MSD including but not limited to detailed diagrams, IP addressing, usernames, passwords, out of band numbers, maintenance contract info, site contacts |
| 15 | PS | Verify and test remote access plan for PBXs (share passwords etc) |
| 16 | PS | Delivery of any failure report to SOMI for all remote access |
| 17 | State of West Virginia | Remediation of all failed remote access |
| 18 | State of West Virginia | Knowledge transfer from existing voice team to MSD |
| 19 | State of West Virginia | Site Preparation |



| | | |
|---|---|---|
| 20 | VZ Field Services | Complete Site Survey Document |
| 21 | Field Services / Account Team | Identify Gaps in Site Survey Documentation |
| 22 | PM / Field Services / PS | Make contact with Site Manager |
| 23 | State of West Virginia | Grant Temporary PBX Password Access |
| 24 | PS | Verify Access to each PBX |
| 25 | PS | Verify Access to VoiceMail System at each site |
| 26 | PS | Analyze PBX Information |
| 27 | PS | Analyze Voice Mail Information |
| 28 | Field Services | Site Visit |
| 29 | Field Services | Site Services to verify physical layout of site voice equipment |
| 30 | State of West Virginia / Account Team | Resolve Gaps in PBX, VoiceMail and Site Surveys |

## Unified Communication and Collaboration Delivery Framework:

Verizon uses a structured approach called the Unified Communications and Collaboration Delivery Framework including the activities needed to prepare, plan, design, and implement Unified Communications and Collaboration services. The UC&C Delivery Framework deploys UC solutions to Verizon customers, helping them improve productivity and increasing effectiveness through the use of repeatable, yet customizable and scalable, tools, templates, and processes specifically developed for UC.

Prepare. The Prepare phase is focused in large part on creation of the business case, This output financial investment, and the technologies involved. From these inputs, the business case is built and a technology strategy is developed along with the high-level architecture to meet those needs with the scope of work.

## Plan

In the plan phase, the Verizon UC Delivery Framework approach helps to assess the existing environment to determine whether it can support the proposed solution. This is done via a series of interviews that includes Account team, Implementation team, and Customer.

### Design

In the design phase, the Verizon UC Delivery Framework approach helps to develop a comprehensive detailed design via a series of workshops with customer and implementation team.

### Implement

In the implement phase, the Verizon UC Delivery Framework approach uses repeatable, yet customizable processes for implementation that were developed and agreed upon in the planning and design phases. UCCaaS solution implementation is managed by the UC PDIS team, an organization chartered to manage project delivery from coordination of Pre-Sales validation through

Post-Sale Operational handoff of UC solutions following the Cisco Prepare, Plan, Design, Implement, Operate and Optimize (PPDIOO) methodology. This organization performs the design, engineering center. UC PDIS confirms appropriate timing for resource implementation on-site in the event that any rack and stack, in person training, or phone placement activity is required. The primary billing structure for UCCaaS is on a per month, per user basis

Verizon UCCaaS is delivered out of our geo-redundant data centers in the 3 regions of the world. Standard time for build-out of each core (which will be completed concurrently) is approximately 6-8 weeks. Once this is complete, the 1st location will be ready for migration.

Verizon will then staff a dedicated team of Project Managers, Order Managers, Engineers, and other pertinent personnel to support the mutually agreed upon migration schedule. Site migrations are performed Monday through Thursday with Friday being designated for the delivery teams to prepare for the following week. In reviewing State of West Virginia's current topology, there are 341 locations and 43,000 users. This equates to approximately 88 weeks of site build/cut activities and would include 60 locations per week. Please note this does not allow for any holiday time, potential black-out periods, etc.

## Virtual Contact Center Implementation Overview

### Implementation Process Overview

The published interval for implementing VCC **core*** services is 45-60 business days (if advanced services are ordered, the implementation interval may be extended or require use of a phased approach). The Virtual Contact Center (VCC) implementation team utilizes audio and web-based tools to provide end-to-end project management for all VCC implementations (no onsite services are provided). All projects begin with a review of the overall process and quickly proceed to requirements gathering to determine the criteria and business rules needed to successfully configure ACD, IVR, and multimedia routing for the customer's contact center.

Once the scope of the project is agreed upon, the VCC Implementation Project Manager (IPM) will work closely with the customer's designated administrator(s) to configure the details of the call flow, providing hands-on training throughout the process. Our goal is to work side by side with the customer to help them learn and understand all the components involved with their VCC application. This will allow them to manage and grow VCC for future business needs. When the scripting is complete, the VCC Implementation Team will test the VCC configuration prior to handing off to the customer for independent User Acceptance Testing (UAT).

To ensure that all VCC users are prepared for the transition to VCC, extensive online training resources are available for on-demand review and train-the-trainer training is provided for the customer's designated trainer(s). On the agreed upon go-live date, the VCC IPM coordinates all cutover activities and ensures that calls are being delivered to VCC agents.

A 10-business day monitoring period follows the cutover. During this time the VCC IPM will remain engaged to address any post-cutover issues that may arise and answer questions as needed prior to the formal handoff to Virtual Contact Center Support.

***Core VCC services are described as voice, e-mail, chat, web callback and click-to-talk. No advanced services (e.g. WFM, QM, CRM integration, etc.) are included.**

## VCC Implementation Roles and Responsibilities

VCC IPM will matrix-manage the VCC implementation inclusive of the tasks identified below, along with the development of appropriate supporting documents. All activities are conducted remotely utilizing conference calls and net meeting to facilitate communications. No onsite services are provided.

- Host discovery session with customer and Verizon Sales Team to confirm contact center data provided, set implementation expectations, review the solution overview, project timeline and roles and responsibilities.
- Conduct weekly status calls with customer and Verizon Teams from project kick-off to cutover.
- Configure the routing script(s) at a level sufficient for discussion and review and inclusion in the Scope Summary document, which will be provided to the customer for approval. The implementation effort will cover the contact types the customer ordered (voice, e-mail, chat). Customer written (email) approval/agreement of the Scope Summary will be required to proceed.
- Provide a training overview document outlining the training resources available for the customer. These resources include online instructor led sessions via web meeting and audio bridge, video tutorials and online help files.
- Provide access to the customer's VCC Business Unit once the Scope Summary is approved in writing by the customer.
- Schedule configuration sessions with the customer to complete the detailed scripting while providing hands-on administrative training sufficient for the customer to be able to handle the post-handoff, day-to-day activities associated with maintaining their Virtual Contact Center.

- Validate the functionality of the scripting in regards to properly handling customer contacts as outlined in the Scope Summary.
- Remotely conduct up to two train-the-trainer sessions on agent and supervisor functionality. Each of these sessions will be limited to three of the customer's designated trainer(s) in each session.
- Work with the Verizon Account team to facilitate a successful cutover to VCC.
- Periodically monitor the customer's VCC application for a period of 10 business days following cutover.
- Provide a review session with the customer on the VCC support portal and the support process for knowledge transfer of opening, tracking and resolution of cases (trouble tickets).
- Host a hand-off call to transition the customer to VCC support upon completion of the 10 business day monitoring period.
- Provide the following supporting documentation during the implementation process
  - Weekly Meeting Minutes
  - Scope Summary/Business Requirements Document (BRD) for Adv. Svs.
  - Project Schedule
  - Hand-Off Document

## VCC Customer Roles

**Administrator(s)** – personnel assigned to participate in VCC configuration meetings to set up VCC security profiles and settings, and configure call routing via scripting sessions, perform baseline configuration of VCC business unit (hours of operation, profiles, points of contacts, etc.) and perform/coordinate user acceptance testing.

**IT & Network Support** – ensure customer environment is enabled for VCC use – order DIDs for agents, open network ports/firewall settings, ping test, FTP site for recording downloads, staff pc requirements, download software, admin rights for specific individuals.

**Contact Center Manager (decision maker)** – approve new VCC call flows, agent and supervisor settings, call reporting, define teams/skill groups, alternate routing requirements, receive outage notifications.
**Trainer** – personnel assigned to attend VCC Train-the-Trainer sessions in order to train agents & supervisors on VCC contact handling.

**Incident Manager** (often assigned to the Administrator or a Contact Center Manager) – manage the VCC support site set up, report incidents impacting VCC service, configure other support users, etc..

**Test Staff** – coordinate and conduct user acceptance testing prior to cutover

**Project Manager** – while not a required role, for large or complex implementations this can be key to ensuring that customer key deliverables are met and project timelines adhered to. For these types of implementations, the customer's designated VCC Administrator may not be able to handle configuration and project management type responsibilities in a matter sufficient to facilitate the success of the project.

** Depending upon your organizational structure, a single individual may act in more than one role.

Customer will:

- Provide at least one, but not more than three, dedicated technical resource(s) (referred to as the VCC Administrator(s) to implement and configure the VCC product. This resource(s) must have strong telephony/technology skills and be capable of understanding and configuring the VCC product.
- Ensure that designated VCC Administrator(s) and other involved personnel are able and available to work with the assigned VCC IPM throughout the process and will complete their assigned tasks independently and in a timely manner.
- Ensure that assigned VCC Administrators(s) will configure VCC to meet the customer's business needs.
- Certify that all premise components (Workstations/PC's, LAN/Internet, phone, etc.) meet system requirements as described in VCC System Requirements document or as advised by the VCC IPM during implementation.
- Perform any necessary modifications/configuration changes relating to premise equipment including but not limited to Workstation Browser settings, LAN(s), PBX, and phones to ensure compliance with requirements.
- Perform independent User Acceptance Testing, notifying the VCC IPM in writing of any specific defects identified. Provide email notification to the VCC IPM when UAT is complete.
- Ensure that each VCC user (anyone receiving any kind of interaction via Virtual Contact Center) has a DID or POTS (unique 10-digit number that terminates to their phone) and a unique email address.
- Ensure that your assigned VCC Administrator(s) will attend a 2-hour Verizon Virtual Contact Center Administration Manager Overview Training session.
- Be prompt to and attend kickoff, weekly project update, and handoff calls.

- Adhere to the defined project schedule so as not to delay the project completion. ****Note that excessive customer delays may require the project to be put on hold and returned to the queue for reassignment when a VCC PM is available and the customer resources are available to proceed efficiently.*
- Notify the VCC IPM and your Verizon Account team of any project impacting delays in a timely manner.
- Independently test and accept the VCC configuration.
- Conduct training sessions to ensure that all Supervisors and Agents handling VCC interactions are adequately trained prior to cutover.
- Complete other internal tasks necessary to begin taking live traffic.
- Use the VCC Support Site documentation to ensure proper service reporting procedures. (This document will be provided in the Handoff Document delivered at the end of the implementation.)

## 3.2 Constraints and Assumptions

The Project Team's ability to meet the defined scope will be based upon the constraints and assumptions outlined below.

- Implementation will commence after receipt of letter of intent (LOI) or Contract Effective Date
- Detailed planning and agreement will be required in collaboration with State of West Virginia
- Additional changes and assumptions may be agreed during the Discovery process
- Implementation is subject to site survey results and Discovery.
- Implementation in certain countries may be dependent on legal and regulatory constraints.

## 3.3 Scope Change Management

Changes to any of the above constraints and assumptions may constitute a change to the overall project. Such changes could impact the project schedule or the ability for the Project Team to provide the agreed upon services to State of West Virginia. Changes to constraints and assumptions will be presented to the Transition Change Management Team for consideration. The Transition Change Management Team includes personnel from both State of West Virginia and Verizon.

# 4 Transition Timeline

## 4.1 High-Level Transition Activities

Verizon has developed a transition approach that includes a methodology that provides for risk mitigation and adequate back out procedures, while minimizing exposure to potential interruptions. This approach allows for the efficient transition to a Verizon-based platform, so that State of West Virginia can quickly realize the financial and operational benefits of the new relationship.

The principal activities involved in the transition from the Current State to the Steady State are:

- Conduct a Discovery data gathering and validation effort
- Establish a Governance structure
- Agreed Transition Plan and key milestones between Verizon and State of West Virginia
- Order and install Steady State Services
- Finalize Steady State service and control management processes

Appendices below show a synopsis of the milestones and associated functions that comprise the building blocks of the overall transition effort. These dates and plans can be reviewed and adjusted based upon State of West Virginia requirements, priorities, and detailed planning. The final scope will also be dependent on feedback and contract negotiations with State of West Virginia. These defined phases may be parallel or overlapping based upon detailed planning and requirements.

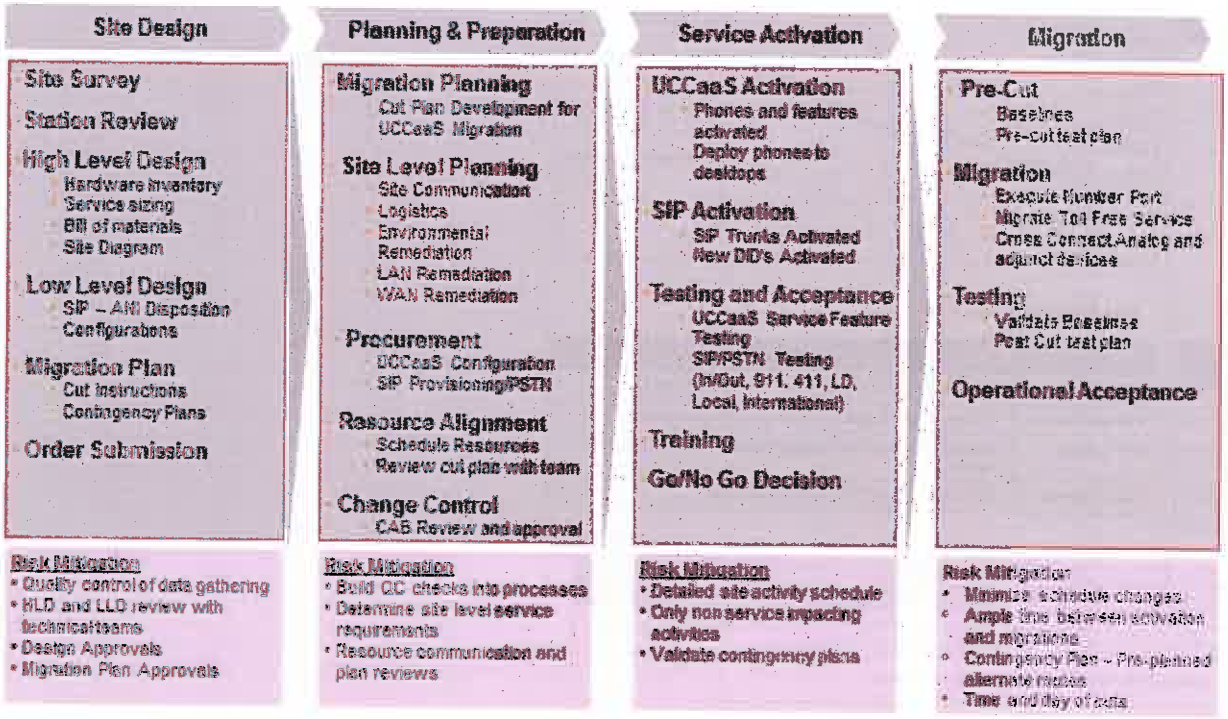
Verizon will work closely with State of West Virginia financial team to identify potential savings and to target a schedule to maximize this benefit while mitigating any and all risks associated with such transition.

## 4.2 Detailed Work Breakdown Structure (WBS)

See High Level Preliminary Project Gantt chart. This will be reviewed and updated based upon detailed planning between Verizon and State of West Virginia. Timelines and schedules can be altered based upon requirements, priorities, and collaborative planning between Verizon and State of West Virginia. Baseline was developed in accordance with the high level dates outlined in the RFP.

Included below is a sample site migration plan which outlines standard steps in the process. Also shown is a sample of the project management dashboard which is used to monitor and control progress throughout the deployment.

## Sample UCCaaS Site Migration Flow



**Site Design**

- Site Survey
- Station Review
- High Level Design
  - Hardware Inventory
  - Service sizing
  - Bill of materials
  - Site Diagram
- Low Level Design
  - SIP – ANI Disposition Configurations
- Migration Plan
  - Cut Instructions
  - Contingency Plans
- Order Submission

Risk Mitigation
- Quality control of data gathering
- HLD and LLD review with technical teams
- Design Approvals
- Migration Plan Approvals

**Planning & Preparation**

- Migration Planning
  - Cut Plan Development for UCCaaS Migration
- Site Level Planning
  - Site Communication
  - Logistics
  - Environmental Remediation
  - LAN Remediation
  - WAN Remediation
- Procurement
  - UCCaaS Configuration
  - SIP Provisioning/PSTN
- Resource Alignment
  - Schedule Resources
  - Review cut plan with team
- Change Control
  - CAB Review and approval

Risk Mitigation
- Build QC checks into processes
- Determine site level service requirements
- Resource communication and plan reviews

**Service Activation**

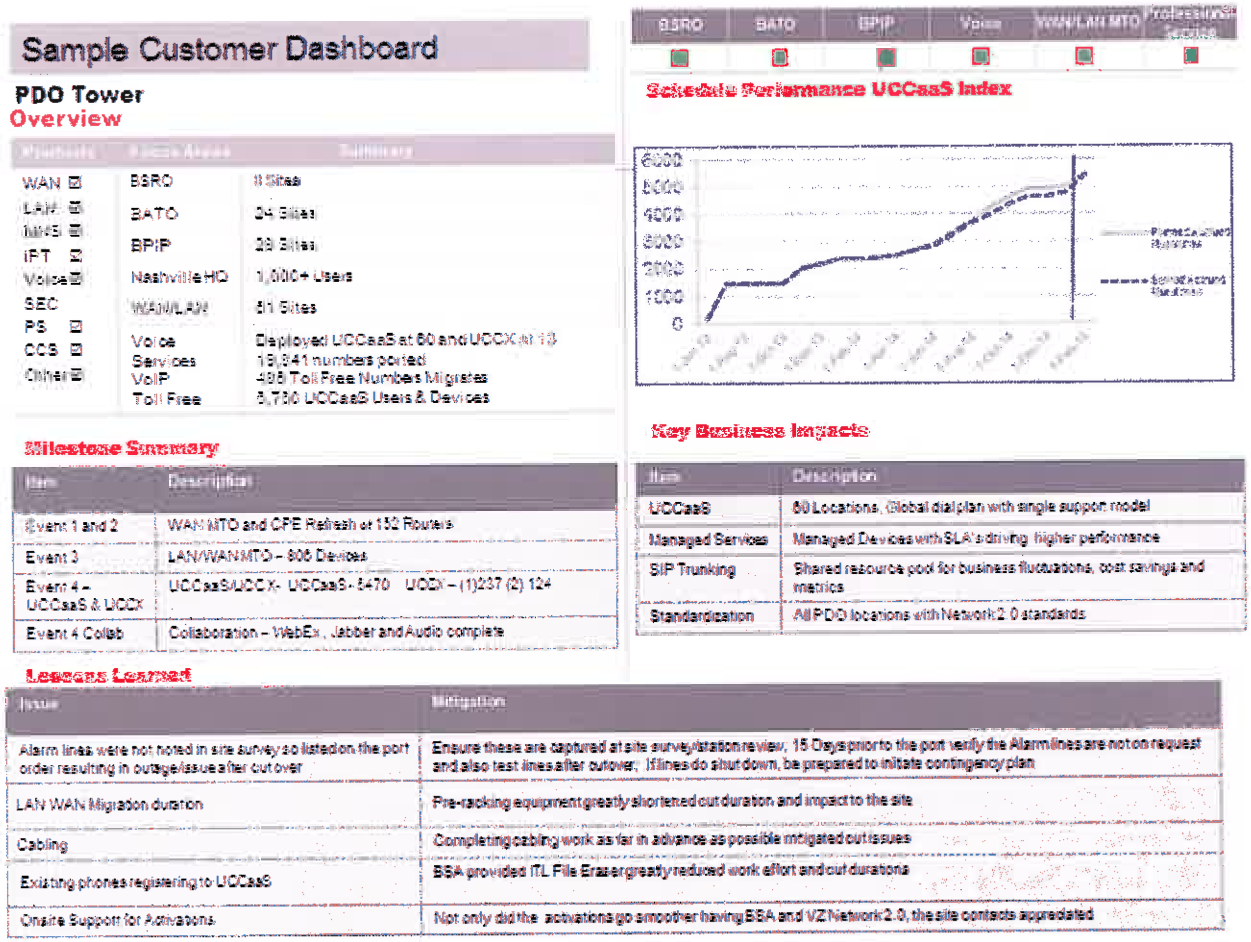
- UCCaaS Activation
  - Phones and features activated
  - Deploy phones to desktops
- SIP Activation
  - SIP Trunks Activated
  - New DID's Activated
- Testing and Acceptance
  - UCCaaS Service Feature Testing
  - SIP/PSTN Testing (In/Out, 911, 411, LD, Local, International)
- Training
- Go/No Go Decision

Risk Mitigation
- Detailed site activity schedule
- Only non service impacting activities
- Validate contingency plans

**Migration**

- Pre-Cut
  - Baselines
  - Pre-cut test plan
- Migration
  - Execute Number Port
  - Migrate Toll Free Service
  - Cross Connect Analog and adjunct devices
- Testing
  - Validate Baselines
  - Post Cut test plan
- Operational Acceptance

Risk Mitigation
- Minimize schedule changes
- Ample time between activation and migrations
- Contingency Plan – Pre-planned alternate routes
- Time and day of cuts



## Sample Customer Dashboard

**PDO Tower**

**Overview**

| Products | Focus Areas | Summary |
|---|---|---|
| WAN ☑ | BSRO | 8 Sites |
| LAN ☑<br>MNS ☑ | BATO | 34 Sites |
| iPT ☑ | BPIP | 29 Sites |
| Voice ☑ | Nashville HQ | 1,000+ Users |
| SEC | WAN/LAN | 81 Sites |
| PS ☑<br>CCS ☑<br>Other ☑ | Voice<br>Services<br>VoIP<br>Toll Free | Deployed UCCaaS at 60 and UCCX at 13<br>19,341 numbers ported<br>498 Toll Free Numbers Migrates<br>5,780 UCCaaS Users & Devices |

| BSRO | BATO | BPIP | Voice | WAN/LAN MTO | Professional Services |
|---|---|---|---|---|---|
| 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |

**Schedule Performance UCCaaS Index**

**Milestone Summary**

| Item | Description |
|---|---|
| Event 1 and 2 | WAN MTO and CPE Refresh of 152 Routers |
| Event 3 | LAN/WAN MTO – 806 Devices |
| Event 4 – UCCaaS & UCCX | UCCaaS/UCCX- UCCaaS- 5470 UCCX – (1)237 (2) 124 |
| Event 4 Collab | Collaboration – WebEx , Jabber and Audio complete |

**Key Business Impacts**

| Item | Description |
|---|---|
| UCCaaS | 60 Locations, Global dial plan with single support model |
| Managed Services | Managed Devices with SLA's driving higher performance |
| SIP Trunking | Shared resource pool for business fluctuations, cost savings and metrics |
| Standardization | All PDO locations with Network 2.0 standards |

**Lessons Learned**

| Issue | Mitigation |
|---|---|
| Alarm lines were not noted in site survey so listed on the port order resulting in outage/issue after cut over | Ensure these are captured at site survey/station review, 15 Days prior to the port verify the Alarm lines are not on request and also test lines after cutover, If lines do shut down, be prepared to initiate contingency plan |
| LAN WAN Migration duration | Pre-racking equipment greatly shortened cut duration and impact to the site |
| Cabling | Completing cabling work as far in advance as possible mitigated cut issues |
| Existing phones registering to UCCaaS | BSA provided ITL File Eraser greatly reduced work effort and cut durations |
| Onsite Support for Activations | Not only did the activations go smoother having BSA and VZ Network 2.0, the site contacts appreciated |

## 4.3 Team Roles & Responsibilities

The Functional responsibility lists outlined below are not exhaustive. Teams should feel free to expand the scope of the responsibilities after consultation between State of West Virginia and Verizon.

### Transition and Transformation Manager

During the Transition period, Verizon will provide one dedicated Transition Manager. The Transition Manager's roles and responsibilities are:

- Act as the initial point of escalation for Services Implementation.
- Develop and provide status reports covering Services Implementation status.
- Assure timely delivery of the Implementation Deliverables and performance of the Services Implementation.
- Secure and manage all resources necessary for Services Implementation execution. Ensure Day 2 Support organizations are trained and able to support State of West Virginia's environment utilizing the Transition and Transformation periods for ramp, training and documentation.
- Lead development of processes and procedures required for Services Implementation and aid Program management in development of the business processes for incident, change, asset, problem, financial and third party vendor management. Establish communications plan, inclusive of governance and escalation guidelines in support of services transition and business transformation with State of West Virginia and Verizon.
- Manage and escalate any outage and performance issues during Implementation to State of West Virginia, Verizon or third party suppliers, and supports remediation process.
- Oversee the completion of all Transition and Transformation 'Towers' and respective tasks with interdependencies in accordance with both Transition and Transformation plans. .
- Document open action items and status reports and conduct post mortems.
- Host status meetings and conference calls regionally and corporate wide, as required.
- Participate in State of West Virginia Governance Committees as outlined in the Agreement.

### Lead Project Manager

Verizon will assign a dedicated Project Manager for the duration of Transition and Transformation. The Project Manager will act as the key transition facilitator during the implementation phase, coordinating all phases of implementation to ensure smooth and efficient transition from the current project environment to a Verizon managed environment. The Project Manager will work closely with the customer to develop the Transition Plan. The Transition Plan will include schedule development, site identification, task identification, inventory conversion and project plan development.

### Key Responsibilities

The Project Manager has the following key responsibilities:

- Execute and maintain project management processes in the areas of project schedule, quality management, communications management, risk/issue management, and change management.
- Develop and maintain project schedules and calendars with the input and assistance of transition leads
- Facilitate team meetings, providing meeting minutes and action items where needed
- Build strong communication channels with internal stakeholders in various departments: Sales, Professional Services, IT Operations, Development teams, Release Management, Networking
- Track tasks assigned to the project team and prepare regular status reports
- Responsible for tracking project changes and producing updated schedules
- Influence continuous improvement of project management methodologies including: assessment of project delivery capabilities, gathering and reporting performance metrics, establishing corresponding targets, and measurement of on-going progress.
- Ensure smooth communication within the project team and other cross-functional teams
- Interface with internal/external stakeholders on a regular basis
- Prepare and document Day 1/Day 2 support documentation and acceptance criteria

### Tower Leads, Project Manager (Cisco UCCaaS)

The Verizon Project Manager has bottom line accountability for the successful completion of the project. The PM responsibilities include:

- Perform overall Project Management services for the implementation of the State of West Virginia Project.
- Develop the Microsoft Project Plan jointly with Verizon support groups and State of West Virginia.
- Distribute and manage the Project Plan, Progression log, milestone tracking and OAI spreadsheets.
- Identify and matrix-manage all resources necessary for project implementation through project completion and acceptance.
- Ensure Transition jeopardies are highlighted on a weekly basis with a Risk mitigation plan and register. Escalate outstanding risks that seem likely to impact schedule/Gateway milestones.
- Oversee the completion of all steps in the defined implementation processes and escalate as needed to insure completion on the projected dates.
- Host and facilitate weekly internal project status call, customer project status call and the project close out call.
- Document and distribute meeting notes and open action items for both the internal and customer implementation project calls.
- Project point of escalation for Verizon and State of West Virginia for the overall project.
- Prepare and distribute the close out / transition document.
- Chair project close out / transition call.

### Project Coordinators - UCCaaS Order Management

The Project Coordinators are responsible for:

- Tracking Order through VRD to Order completion
- Order Verification with Customer
- Conduct Stakeholder Communication (Customer & Verizon)

- Manage Order Jeopardy & Escalation Management
- Submit UOTM email to customer to confirm order
- Maintain order status in EZstatus
- Provide standard tracker to customer
- Maintain schedule of implementation and completion logs and integrate status into the Transition PM's progression log for consolidated distribution.
- Serve as second-level escalation point for activation/migration issues

### Service Desk/e-Bonding/Tools Lead

The Service Desk / e-Bonding Lead is responsible for:

- Identifying Key Contributors/SMEs.
- Scheduling data mapping sessions with Verizon and State of West Virginia Remedy engineers.
- Clarifying fields' intent, categories and ensuring Verizon e-Bonding developers understand State of West Virginia's use of specific fields that need to 'map' into Verizon's incident management system, (ETMS).
- Clarify connectivity requirements, Citrix/Access and testing with Service Desk
- Document/Diagram Processes for incident, service requests and changes utilizing the e-Bonded appliance tool or other integrated tools
- Identify incident, change and service request categories/types for routing to specific Resolver Groups. Establish Work Level instructions to aid PMO, and other organizations (Verizon, TPVs, Carriers, State of West Virginia) to
- Develop test scenarios and pilot testing before 'go live', coordinate testing with State of West Virginia, and coordinate in any revisions, if required. Implement e-Bond and monitor incident routing/resolutions and ticket status updates with State of West Virginia and Verizon developers.
- Establish Business Continuity Plan for Tools and systems that Verizon and State of West Virginia utilize in support of the Services (ETMS/HP Service Manager, Change Management, Asset Management, SharePoint, etc.)

- Ensure Verizon adheres to service deliverables, ticket status/assignments, routing and escalation in accordance with the Agreement and the Process and Procedures Manual. Modify instructions/training, as indicated, to meet service objectives per the Agreement
- Coordinates all aspects of Service Desk Implementation
- Facilitates activities among cross-functional teams and customer
- Ensure that requirements have been identified, documented and agreed upon with all key stakeholders
- Communicate the expectations and deliverables to each of the teams responsible for owning, enabling and implementing eBonding
- Facilitate the readiness of process dependencies, major deliverables and milestones against the Service Transition charter and Implementation Project Plan
- Ensure the agreed upon handoffs between accountable teams
- Manage the overall implementation, testing, acceptance and handoff to the customer

**UCCaaS Delivery Team**

**UCCaaS Engineer:**

- Design and deliver UCCaaS solution,
- technical project lead,
- Create LLD, configure apps and users, system testing, provide Day 1 support.

**UCCaaS Delivery Coordinator:**

- Coordinate Verizon teams and customer to execute UCCaaS SOW/SOR,
- Manage UCCaaS deliverables, customer communications,
- Build UCCaaS implementation schedule,
- Complete UCCaaS orders, user training, staging and data collection coordination.

**End-User Feature Trainer:**

- Trains your train-the-trainers on end-user features such as desk phones, SmartOffice UC Client

**CUCDM Admin Training:**

- Trains your administrative personnel on the CUCDM admin portal.

**UCCaaS Service Desk:**

- Provide Day 2 support (MACD and fault management).

### Steady State - Day 2 PMO

**Program Delivery Manager**

**Responsibilities**

The Verizon Team will be led by a Program Delivery Manager who is selected for State of West Virginia because he or she has a proven track record of performance in managing numerous project teams simultaneously and in understanding that State of West Virginia's business. The Program Executive will work closely with, and coordinate the efforts of, Verizon' Project Managers and Operations Managers and State of West Virginia's stakeholders in developing joint plans and schedules with regularly scheduled reviews. This type of relationship from the beginning creates a partnership between Verizon and State of West Virginia for all activities planned and performed in State of West Virginia's organization. State of West Virginia will play a key role as a partner on the team—participation of State of West Virginia's staff is critical to the success of all projects.

- Oversees and Manages the Verizon/State of West Virginia Contract for contracted solution and services.
- Acts as primary liaison between the Verizon project team and State of West Virginia.
- Acts at the "glue" across all resources and support organizations within Verizon required to deliver the solution.
- Monitors ongoing service management to ensure compliance with SLAs and performance commitments.
- Engages with Operations to communicate, and/or escalate on any outage and/or performance issues to Verizon and State of West Virginia.
- Monitors resource load and distribution to ensure the quality delivery of services.

- Ensures that all contracted program deliverables are completed.
- Facilitates long range business planning meetings with the Account Team and State of West Virginia, in support of State of West Virginia' long term business strategies and plans.
- Participates in any technical, network, SLA, contract compliance escalation as appropriate. Engage with State of West Virginia executives and Verizon executives in the prioritization and resolution of escalations, as appropriate.
- Establishes periodic status meetings with State of West Virginia, Verizon and any Third Party Vendors to discuss status of contractual relationship.
- Presents a formal monthly program review for State of West Virginia, examining all aspects of the Verizon solution in the previous month, highlighting successes and failures, and recommending measures for improvement.
- Assists Account Team in fielding any business and/or technical requests and engage the appropriate internal Verizon resources.

### Financial Services Manager

During the Term, Verizon will provide one full time dedicated Financial Service Manager. The FSM's responsibilities are as follows:

- Document the agreed-upon billing and invoicing process and invoice format;
- Manage Verizon's compliance with the billing and invoicing process;
- Deliver supplementary invoice reports (in Excel or CSV format) to State of West Virginia Global in a form mutually agreed upon between State of West Virginia and Verizon;
- Manage billing questions, inquiries, and disputes to resolution;
- Manage Verizon's request(s) and the processing and issuance of SLA credits, as appropriate;
- Assist State of West Virginia in setting up billing structure;
- Review New Services billing for accuracy;
- Report on State of West Virginia AVC attainment;
- Track credits due to State of West Virginia;

- Partner with Verizon Project Managers and provide a forecast of upcoming charges to State of West Virginia;

### Service Level Management

During the Term, Verizon will provide one full time dedicated Service Level Management Reporting Analysts. The Service Level Management Reporting Analysts will perform the following responsibilities:

- Review Verizon's contract performance for compliance with the terms of the Agreement, including monitoring of all minimum volume commitment thresholds. Report results in the monthly meeting;
- Facilitate communication between State of West Virginia and Verizon executives, including the escalation of State of West Virginia or Verizon performance issues as required;
- Monitors ongoing service management to ensure compliance with SLAs and performance commitments.
- Prepares performance reports and service level reports; these reports will collectively show Verizon's compliance or degree of non-compliance with service levels and compliance with associated performance requirements.
- Maintains a repository of performance reports provided.
- Manages dashboard reporting, as mutually agreed to with the client and documented in the Process and Procedures Manual.
- Cooperates with the client to assess service level and other contractual remedies; initiates and manages the process of service credit requests based on non-compliant performance with respect to signed agreement.
- Ensure that improvement initiatives identified in Service reviews are acted on and updates are provided to State of West Virginia;
- Ensure that changes are assessed for their impact on Service levels;
- Identify opportunities for Service improvement and risk mitigation and engage appropriate State of West Virginia and Verizon resources to address those opportunities and develop Service Improvement Plan (SIP) as appropriate

### Cisco UCC Lead Architect

Verizon will assign one fulltime dedicated Cisco UCC Lead Architect.

The Cisco Unified Communications (UC) lead architect will support the transformation project to act as a technical advisor on the preparation, planning, design, implementation, integration, and operations of UC environment.

This resource will be an overall technical lead in the architecture planning, design, implementation, and operations of the UC solution.

The enterprise architect will provide in-depth UC subject matter expertise and guidance to executive management as well as other stakeholders responsible for the positioning, planning, and delivery of UC services within the State of West Virginia.

The Cisco UCC enterprise architect will have:

- In-depth knowledge and demonstrable experience in designing and implementing switching and routing protocols, Quality of Service (QoS), Internet Protocol (IP) Private Branch Exchange (PBX), and Session Initiation Protocol (SIP) on an enterprise level.
- Expertise in designing, implementing, and maintaining complex Voice over IP (VoIP) call control, call routing, and applications and services with a specific skillset around **Cisco UCM**.
- Ability to define UC processes and procedures and develop work plans.
- Ability to exercise judgment within defined procedures to determine appropriate action.
- Ability to communicate effectively both verbally and in writing.
- Ability to summarize technical concepts and communicate to senior-level management.
- Ability to work effectively with and provide guidance to other members of the work group.
- Provide oversight of MACD changes to the UC environment.

- Specifically design and ensure security of integration issues related to the telecommunications network or related network services
- Participate in the analysis, design and planning, and implementation of State of West Virginia-related systems supported under this contract
- Provide technical expertise in all State of West Virginia design improvement and security
- Identify opportunities to improve business processes by building on existing/new technologies and applications
- Prepare and maintain high level infrastructure and application's documentation in support of project requirements and operations.
- Plan, build, test and deploy appropriate infrastructure solutions and configurations

  - Conduct due diligence on equipment and service proposals
- The Cisco UCC lead architect will lead all design and implementation rollouts for any lab, pilot, and production-related cutovers.
- This resource will represent the State of West Virginia administrator role of an UCCaaS environment. This administrator will interact with the Verizon UCCaaS service desk for standard and optional MACDs.
- The Cisco UCC lead architect will be familiar with all Verizon UCC products related to the UCCaaS deployment, including Verizon UCCaaS, IP Trunking, Managed Network Services, and Private IP circuits.

# 5 Communication and Documentation

Project Communication Management is the process that specifies how and when team members communicate and share information with one another and with others outside the project team.

## 5.1 Project Communication

Transition planning meetings will be conducted during the initial stage of transition to review task and activity plans, transition deliverables, and to establish the project baseline. Verizon anticipates that State of West Virginia will participate in all transition planning meetings. These meetings will be scheduled at mutually agreed upon times and frequency until the final project baseline is established. Weekly project status meetings will be scheduled at mutually agreed upon times, where the Verizon Transition Team will present the status of the Transition Project Plan along with identified issues. The Verizon Transition Manager will facilitate multiple meetings or workshops to conduct detailed planning with the transition team to:

- Identify key participants in these meetings, including State of West Virginia Program Management staff associated with the transition, Verizon service delivery representatives, project managers, and key third-party vendors
- Define roles and responsibilities of State of West Virginia, Verizon, and other key suppliers
- Identify State of West Virginia priorities and blackout dates and agree to overall timetable and associated milestones
- Sign off on final design and rollout plan
- Identify and address any remaining Discovery work that must be completed prior to initiating transition or transformation
- Identify and validate all remaining assumptions
- Finalize and communicate the complete timeline, milestone, and deliverables schedule for the transition and transformation

The deliverables from the transition planning workshops are:

- ✓ **Transition Teams:** Identify all the key managers and work staff, with a clear understanding of tasks and responsibilities

- ✓ **Transition Plan** that includes process integration and implementation plan, vendor management plan, and knowledge transfer.

Verizon will establish conference calls for the duration of the project providing a forum for communication, review, and discussion of open actions items, issues, thoughts and concerns.

## 5.2 Project Documentation

During this transition project, multiple documents will be passed between Verizon and State of West Virginia, updating the team on weekly progress. Examples of standard transition documentation are listed below.

***Transition Project Plan*** – The sequence and timeframes detailed in this document are based upon information gathered by the Verizon Account Team and Project Manager, and dates proposed in the State of West Virginia Transition Schedule. The Verizon Transition Manager owns the Transition Project Plan updates and communication regarding those updates to the project team.
***Weekly Implementation Report and Review*** - The weekly implementation report will be reviewed by the Transition Manager and the customer. Jeopardy items include CPE-related issues, site not ready, power-related concerns, etc.
***Preliminary Network and Equipment Diagrams*** – These documents provide State of West Virginia with the finalized network design. These design documents require formal State of West Virginia engineering review and approval prior to the commencement of each phase of this project.
***Implementation Procedures and Testing*** – This document provides comprehensive implementation and test plans and will serve as historical information for future projects of this type.

The Project Managers for Verizon and State of West Virginia will be copied on all documentation and will be the central points of contact for communication to the project team.

## 5.3 Transition Management Reporting

Verizon will provide State of West Virginia with the following customized and standard reporting during the transition:

- Implementation Status Report
- Green/Blue/Red Identifiers
- Lessons Learned and Action Items List
- Service Level Agreement Status
- Transport (Provisioning) Status

- Third-Party Vendor Activity as required

Verizon Project Managers are equipped with several tools that assist them in managing all types of projects. Most of these tools, including the PM checklist, generic project plans, and product and service Gantt charts, have been developed within the group. These tools are specifically designed to assist in the project management of our large and complex Global Account projects. Microsoft Project and other reporting tools are also used to ensure the project milestones and deliverables are being tracked and reported.

### 5.4 Escalation Management

In the event that, after working with our standard support processes and with our service and PMO teams, State of West Virginia is not satisfied with the timeliness or level of service provided by Verizon, an escalation should be initiated. Escalations may also occur when events impact State of West Virginia production environment, with the potential of causing high risk to business operations.

During the transition process, PMO will refine the list of essential Verizon support personnel and define the escalation hierarchy and processes for specific service areas. Contact information (office, mobile, pager, e-mail) for key management and executive resources within the appropriate Verizon departments will be shared with the State of West Virginia project team.

## 6 Resource Management

### 6.1 Transition Management

At the outset of the Transition phase, Verizon will establish Transition Program Office. Along with these individuals will be Verizon networking professionals who bring strong process, project management, and integration experience.

Project Managers associated with the network are professionally certified and proficient in the use of industry standard tools (*e.g.*, Microsoft Project and GANTT charts) and applicable business methodologies.

The State of West Virginia Designated team will consist of the following members:

- Account Manager
- Transition Lead Project Manager

### 6.2 Transition Team Resources

A successful transition depends upon the efforts of the following key resources:

- Lead Transition Project Manager

- Tower Project Managers
- Implementation/Order Managers
- Implementation Engineers
- Subject Matter Experts

## 6.3 State of West Virginia Project Team Responsibilities

Verizon's ability to meet the project scope and schedule depends on the following State of West Virginia responsibilities during transition:

- Dedicate qualified resources to the Transition Team, including a dedicated team lead, during the entire transition period.
- Provide designated subject matter experts to work collaboratively with Verizon to facilitate Verizon's creation of interfaces for tools/systems/applications and user acceptance and production testing of such interfaces. Ensure subject matter experts are made readily available during the entire transition period.
- Provide Verizon with State of West Virginia blackout dates, hours, and time restrictions for migration of devices to occur with any exceptions noted for staffing/scheduling optimization by Verizon, State of West Virginia, and relevant third-party vendors. Please note that, in order to adhere to a migration schedule, a mutually agreeable procedure for scheduling changes must be established prior to contract signature.
- Provide complete and accurate device list including IP addresses.
- Provide complete and accurate user station information, telephone numbers for porting, and site requirements.
- Reconcile data integrity issues promptly, as needed.
- Provide the Transition Team with appropriate points of contact for on-site facilities.
- Ensure any changes in local contacts/alternate contacts are communicated to Verizon.
- Ensure that all local and alternate contacts are aware of the project, timeframes and scope.
- Provide access and/or licenses for any required customer tools, should any be required, to complete migration activities.
- Provide access to site facilities, if site surveys by Verizon field technicians are required.
- Provide designated subject matter experts for data mapping and testing scenarios to meet tools integration requirements.
- Support scheduling and deployment of tools and enhancements.
- Coordinate transition issues with customer third-party service providers, such as local access providers as required.
- Produce a mutually agreed-to set of metrics as specified in the Transition Plan; these metrics will be used by the Transition Team to measure progress.
- Facilitate transition, project management, and timely issue resolution mechanics through communications with State of West Virginia-identified resources. Specifically, Verizon is requesting State of West Virginia to provide a documented escalation chain to ensure the appropriate business stakeholders are identified.
- Participate in a mutually agreed upon change management process regarding the Transition Services and provide escalation assistance as needed.
- Stabilize network and system devices toward their appropriate security baseline

- Develop and manage security compliance plan and establish best practices and documented procedures for device security administration, and implement device configurations for logging security events and the use of administrative rights, and communicate security processes, configurations, and security data to the Security Team.
- Ensure that accounts on are controlled, authorized, and enrolled though processes that are clear, documented, and approved by the Security Team, and define security configuration for all in-scope components

# 7 Risk Management

It is important to identify and analyze risks to determine which risks pose the greatest threat to the project's successful outcome and to address and treat them as early on in the project as possible. As part of our Risk Management activities, Verizon performs risk analysis, response planning, monitoring and control.

Large projects, such as this one, may require more detailed risk planning due to the number and complexity of risks. This process often includes the development and analysis of alternative strategies and strategy evaluation criteria. The ranking and development of mitigation strategies may also require a larger scale of assignments for probability and/or impact (such as low, medium, high, and very high). In addition, the following sample risk management checklist may be useful tool during risk planning:

| RISK MANAGEMENT CHECKLIST | |
|---|---|
| Is there a process for identifying and documenting risks? | □ |
| Were all phases and aspects of the project taken into account during the risk identification process? | □ |
| Has the exposure of each identified risk been rated? | □ |
| Has a mitigation strategy been identified for each identified risk? | □ |
| Has a contingency strategy been defined for each identified risk? | □ |
| Has a trigger been established for each contingency strategy? | □ |
| Does the project plan include tasks for active monitoring for risks? | □ |
| Is there a process for tracking and reporting on risks? | □ |
| Has the entire project team been apprised of the risk management processes? | □ |

# 8 Governance Model

Verizon places strong emphasis on the importance of an effective multi-tier governance program as a means of ensuring the long term success of a collaborative technology program. We have found that governing from transition to steady state effectively is an essential component of a successful relationship and in managing inevitable changes and unexpected issues. Verizon's intent is to collaborate on the specific design of the Governance Model to meet State of West Virginia specific needs. The Governance model is intended to be flexible and leverage existing State of West Virginia processes.

# 9 Post-Transition Report

Following the execution of the Transition, Verizon PMO conducts a comprehensive review and prepares and distributes to State of West Virginia a Post-Transition Report. This report contains a candid summary of the success of the transition activities and details any follow-up actions that may be required.

# Appendix H. Virtual Communications Express (VCE)

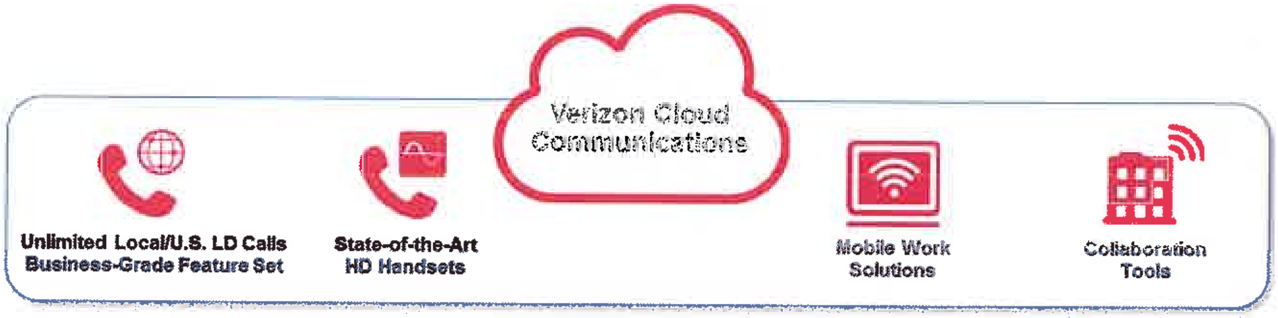
At Verizon we know that your day is filled with business critical work, and you need every advantage to stay ahead of your competition. That's why we created Virtual Communications Express.

Virtual Communications Express is a simple, reliable approach to deliver critical technologies so that The State of West Virginia can confidently focus on business possibilities.

With Virtual Communications Express, you get an end-to-end communications service built for you and delivered from our cloud. You get phone service that is packed full of features that can help make your business more efficient and productive. You get state-of-the art phones, specifically designed for businesses like yours.

You get instant messaging and presence, audio and video conferencing, and desktop and mobile screen sharing that will enable you to collaborate internally and with your customers and suppliers better than ever before.

- Organizations of all sizes recognize the intrinsic importance of voice, Internet, and desktop applications
- Integrated, reliable communications enable responsiveness to customer demands and needs, to create a competitive edge
- The ability to power productivity, foster innovation, and collaborate faster. Management of these technologies should not distract you from your main business focus


Verizon Cloud Communications
Unlimited Local/U.S. LD Calls Business-Grade Feature Set
State-of-the-Art HD Handsets
Mobile Work Solutions
Collaboration Tools

## Enterprise-level Power, Functionality, and Features

Virtual Communications Express is a robust, yet simple “plug and play” or professionally installed solution:

- Benefits and efficiencies of anytime unified communications capabilities across corporate voice and IT systems.
- Ability to boost productivity using existing broadband Internet service or Private IP connections. The State of West Virginia can use the collaborative and mobile tools that Virtual Communications Express offers – i.e. audio and video conferencing – to easily and quickly bring employees or clients together when making decisions.

  Mobile clients can also enable the ability to take calls and conduct conference meetings while on the go. You can remain productive when outside of the office (unlike plain old telephone service), and maintain continuity, so your business can continue to run smoothly.
- Alleviate the effort, complexity, and risk associated with technology management.
- Access leading applications and self-service capabilities.
- Simple installation and activation – no IT expertise required.
- Seamless communication across your organization, right “out of the box”.

## Valued Features, Reliable Support

- “Bring your own broadband” or Secure Private IP Access
- Voice over IP calling; unlimited local and domestic long distance within the U.S.
  - Feature-rich, state-of-the-art phones
  - Standard and optional voice features
  - Carrier-grade, fully redundant platform architecture
- Unified Communications and Collaboration Capabilities
  - Instant Messaging
  - Telephony presence
  - Audio and Multi-point video conferencing*
  - Screen and File Sharing*
  - *to be used with applicable Desktop and/or Mobile client(s)

- Business continuity features
  - Simultaneous ring
  - Mobile clients for Apple iPhone and Android smartphones
  - Automatic forwarding to an alternative number if your locations loses Internet connectivity
- Uncomplicated, cost effective unified communications solution to power productivity, accessibility, and world-class service

Virtual Communications Express is particularly valuable for organizations that:

- Maintain multiple branch or franchise sites
- Have limited local or outsourced IT department support
- Rely on remote or mobile work force
- Expand or contract due to seasonal needs
- Are experiencing rapid growth with a quick to deploy solution
- Demand business continuity features
- Seek to replace aging or outdated equipment without large capital investment

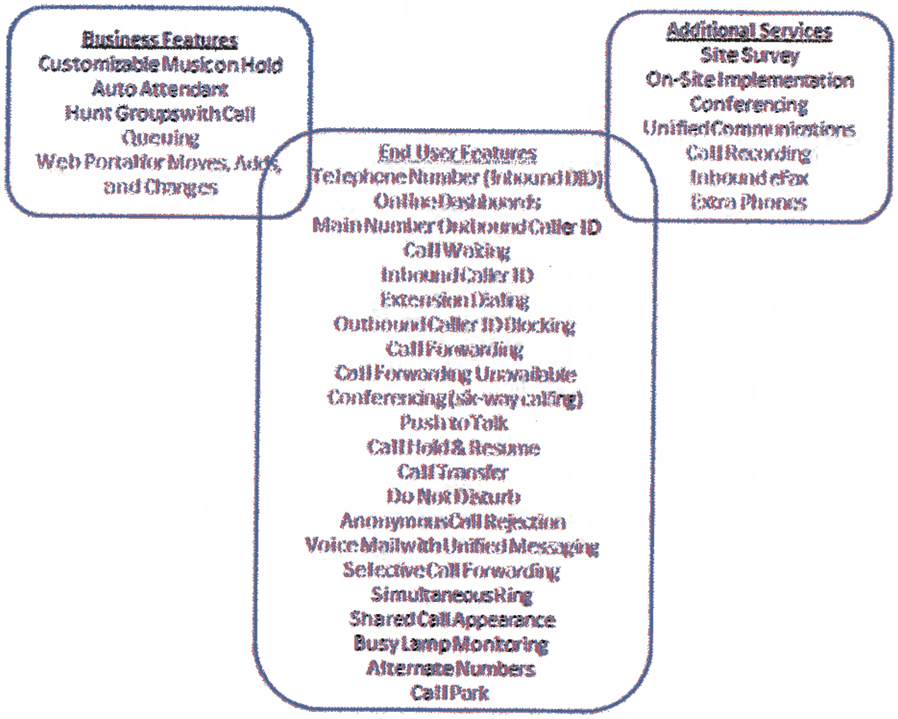
Unify your communications approach quickly, easily, and cost-effectively – and manage it to meet changing demands and complement business growth.

## Features

Virtual Communications Express the State of West Virginia will experience enterprise-grade functionality, which enables key features such as:

- Unified communications, which provides the ability to collaborate with business employees, co-workers, and/or customers via audio and video conferencing, desktop screen sharing, and file sharing. Included for Premier users, and available as on optional add-on feature for Standard users.
- Call Recording, as an optional feature add-on, is an integrated, fully hosted solution to record, store, organize, and access recordings of inbound and outbound calls.
- Simultaneous ringing of multiple devices, such as an office phone, mobile or home office line.
- Voicemail messages and inbound faxes via email.
- Office Anywhere enabling calls to be flipped from an office line to mobile and allowing calls made from a mobile or home phone to show office caller ID.

- Key System functionality, which allows incoming calls to ring on all phones in the office and be answered by any user on any phone.
- Contact Center Agents/Supervisors.

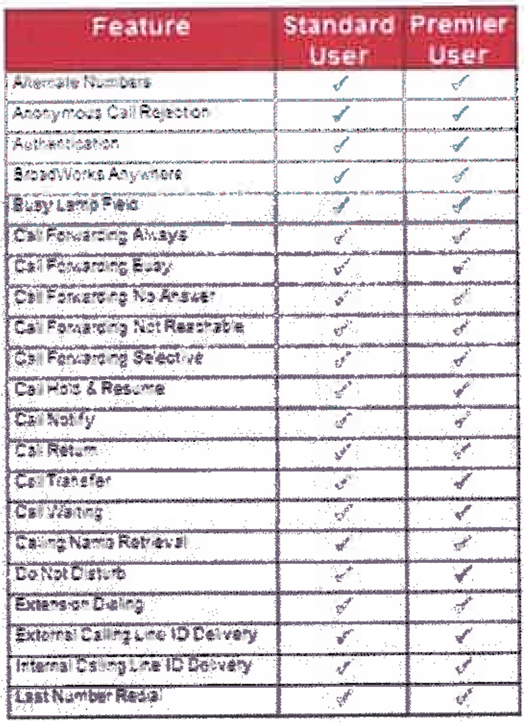


**Business Features**
Customizable Music on Hold
Auto Attendant
Hunt Groups with Call Queuing
Web Portal for Moves, Adds, and Changes

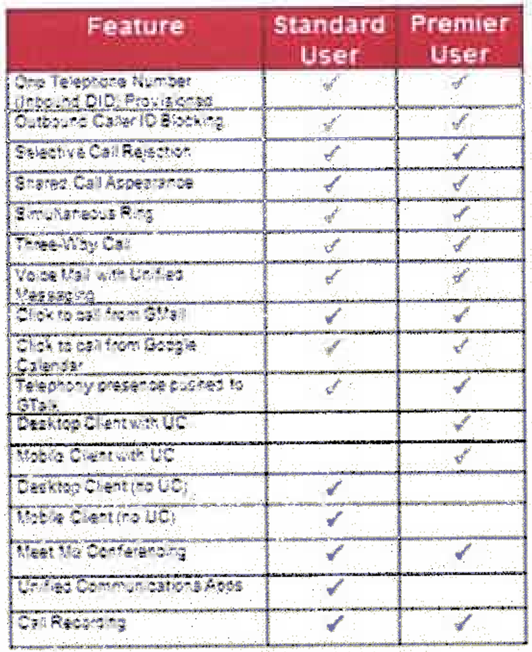
**End User Features**
Telephone Number (Inbound DID)
Online Dashboards
Main Number Outbound Caller ID
Call Waiting
Inbound Caller ID
Extension Dialing
Outbound Caller ID Blocking
Call Forwarding
Call Forwarding Unavailable
Conferencing (six-way calling)
Push to Talk
Call Hold & Resume
Call Transfer
Do Not Disturb
Anonymous Call Rejection
Voice Mail with Unified Messaging
Selective Call Forwarding
Simultaneous Ring
Shared Call Appearance
Busy Lamp Monitoring
Alternate Numbers
Call Park

**Additional Services**
Site Survey
On-Site Implementation
Conferencing
Unified Communications
Call Recording
Inbound eFax
Extra Phones

## User Features



| Feature | Standard User | Premier User |
|---|---|---|
| Alternate Numbers | ✓ | ✓ |
| Anonymous Call Rejection | ✓ | ✓ |
| Authentication | ✓ | ✓ |
| BroadWorks Anywhere | ✓ | ✓ |
| Busy Lamp Field | ✓ | ✓ |
| Call Forwarding Always | ✓ | ✓ |
| Call Forwarding Busy | ✓ | ✓ |
| Call Forwarding No Answer | ✓ | ✓ |
| Call Forwarding Not Reachable | ✓ | ✓ |
| Call Forwarding Selective | ✓ | ✓ |
| Call Hold & Resume | ✓ | ✓ |
| Call Notify | ✓ | ✓ |
| Call Return | ✓ | ✓ |
| Call Transfer | ✓ | ✓ |
| Call Waiting | ✓ | ✓ |
| Calling Name Retrieval | ✓ | ✓ |
| Do Not Disturb | ✓ | ✓ |
| Extension Dialing | ✓ | ✓ |
| External Calling Line ID Delivery | ✓ | ✓ |
| Internal Calling Line ID Delivery | ✓ | ✓ |
| Last Number Redial | ✓ | ✓ |



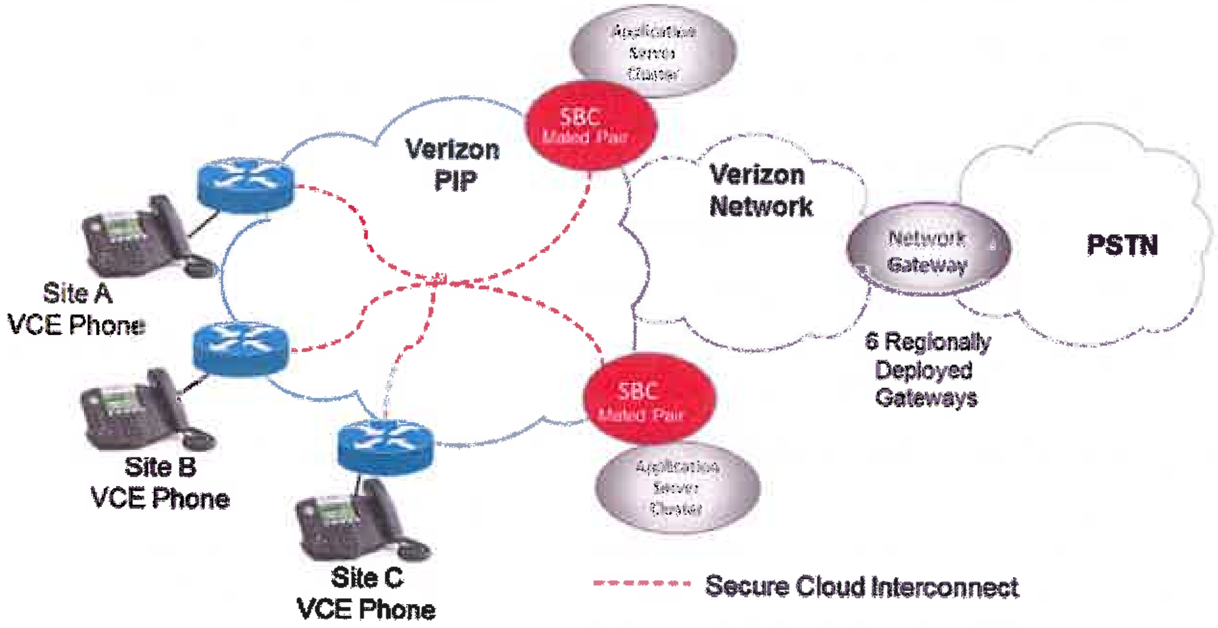
| Feature | Standard User | Premier User |
|---|---|---|
| One Telephone Number (Inbound DID) Provisioned | ✓ | ✓ |
| Outbound Caller ID Blocking | ✓ | ✓ |
| Selective Call Rejection | ✓ | ✓ |
| Shared Call Appearance | ✓ | ✓ |
| Simultaneous Ring | ✓ | ✓ |
| Three-Way Call | ✓ | ✓ |
| Voice Mail with Unified Messaging | ✓ | ✓ |
| Click to call from GMail | ✓ | ✓ |
| Click to call from Google Calendar | ✓ | ✓ |
| Telephony presence pushed to GTalk | ✓ | ✓ |
| Desktop Client with UC |  | ✓ |
| Mobile Client with UC |  | ✓ |
| Desktop Client (no UC) | ✔ |  |
| Mobile Client (no UC) | ✔ |  |
| Meet Me Conferencing | ✔ | ✔ |
| Unified Communications Apps | ✔ |  |
| Call Recording | ✔ | ✔ |

✓ = Included
✔ = Optional

## Virtual Communications Express over Private IP

Virtual Communications Express over Private IP (PIP) enables customers using Verizon PIP services to transport their Virtual Communications Express service across their PIP network.

- PIP connectivity has been put in place between the Broadsoft data centers and our PIP network
- A SCI connection is used to create a logical connection for each customer to those Broadsoft applications



Virtual Communications Express over PIP enables current Verizon PIP for routing through the Broadsoft Cloud PBX Platform so that your voice traffic can be added to the circuit and attains the current SLAs offered for VoIP QoS on the Verizon PIP network and maintain the added security that PIP affords.

### Six Reasons to Switch to Virtual Communications Express

- Helps improve collaboration and productivity – Faster decision-making, better customer service
- Greater Mobility – The same great features available whether in the office or on the move
- Grows with your business – Expand without incurring large equipment costs
- Easy Installation – Out of box, plug and play: Use with any broadband service or Private IP
- Control Communication Costs – Unification of services
- Premium Phones – High-definition voice quality

## Summary

- A robust, resilient hosted solution for your business offering simple, scale-able IP Voice with enterprise-grade power and functionality, such as Unified Communications, inbound eFax, mobile/desktop clients, business continuity, auto-attendant, and hunt groups.
- Polycom IP handsets and option to support Android and Apple smartphones with a mobile client allow single number reach. This means you can be reached via one phone number, whether in the office at your desk or on your mobile phone.
- Combine with Verizon Private IP, Internet access or any 3rd party Internet access.
- Competitive, predictable, flat monthly price per user, which includes the DID, call control features, voicemail, and enterprise-grade features, such as music on-hold, hunt group, auto attendant and call queuing. Polycom phones can be purchased or rented (they are not included in the per user price).
- Limited or no capital investment required.
- Ability to scale up or down for growth or seasonal variation.
- Rapid deployment capability provides the ability for The State of West Virginia to bring on new sites quickly and efficiently.
- Online management portal enables administration of end user accounts.

Getting Virtual Communications Express is easy. The service offers high quality phones, unlimited local and nationwide long distance voice calling, self-service functions, and unified communications capabilities, as well as a means to alleviate the effort, complexity, and risk associated with the management of such technology.

Best of all, buy only what you need, and add new phones as desired. The entire package is backed by Verizon's 24/7 business support.

With Virtual Communications Express the State of West Virginia can focus on what you do best – your core business.

# Appendix I. Account Service Plan

As the Verizon Account Team for State of West Virginia we have a highly experienced workforce of consultants, engineers, and specialists focused on helping you recognize technology's opportunities– empowering you to perform, execute, and grow in new and better ways.

Your Verizon Account Team is available to answer any service or industry related questions and investigate the right mix of new and converging technologies. We want to understand your business and operation objectives to help fully satisfy your expectations.

The following information includes an account relationship plan to provide timely and effective reporting as well as an outline of account team roles and responsibilities, trouble reporting, and escalation procedures.

## Account Management Plan

Verizon is a service company, and we believe all organizations within the company, whether they interface directly with customers or simply provide support to those organizations that do, should be dedicated to providing the best customer experience.

We are continually focused on simplifying key areas of our business to serve you even better, including:

- Customer satisfaction
- Sales effectiveness
- Operating efficiency

We will engage with you strategically in order to understand your business and build a mutually beneficial, long-term relationship.

To achieve this goal, we continue to refine operations so they run efficiently and at high performance levels to deliver excellent service. Because company resources are aligned with our sales and customer support organizations, we're better able to serve you.

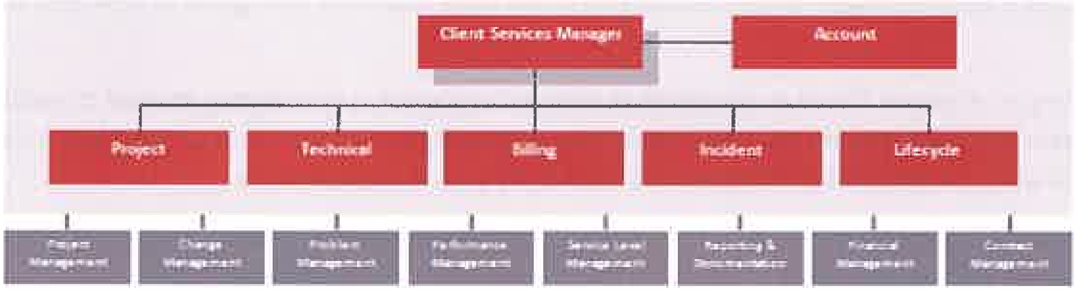
We also understand that the way to deliver an exceptional support experience to State of West Virginia is to empower our sales and service personnel with the resources and tools they need to help you make the best decisions for your business.

Today's emerging solutions require unique skills, capabilities, and support structures that we've built into our support organizations.

We are focused on developing stronger solutions sales capabilities. Our sights are set on being the world's leading platform-based solutions provider, and your ultimate partner to navigate the technology landscape and drive your business.

## Verizon Client Service Team

The chart illustrates the functional organization chart of the Verizon Global Operations Organization. Details of the resources and roles and responsibilities are provided below.



*Verizon Functional Organization Chart*

### Roles and Responsibilities

#### Account Manager (AM)

- Provides solutions from the Verizon product range to help enable the achievement of your business outcomes;
- Serves as the primary sales team interface working in partnership with CSM to grow the partnership and overall relationship between you & Verizon.

#### Solutions Architect

- Solutions Architect will be your technical expert/architect and provides on-going technical engineering support to provide overall engineering oversight of your network, as well as perform engineering activities that are outside the scope of Standard Change Management activities;
- Recommends the network requirements, network design topology architecture and technology upgrades;
- Develops network backup/contingency plans;
- Solutions Architect on-going customer relationship roles:
  - Support and conduct detailed technical presentations for State of West Virginia with account team and other technical resources.
  - Completes internal high level design documents required for provisioning and implementing Customer network design and endures overall high level network design meets mutually agreed upon requirements
  - Provides new site design and existing site upgrades.

  - Research and recommend new networking products that integrate within the existing environment.
  - Design and support Proof of Concept Applications that are Network dependent. Examples would include 4G LTE backup.
  - Engineering Planning Reviews; Hosts weekly meetings with customer to review important topics that need attention. Reviews the performance of the network and evaluates its efficiency (routing and topology).
  - Proactively review & analyze Customer's network for improvements, i.e. upgrades, diversity planning, disaster recovery & other network improvements.
  - Proactive optimization of existing network resources and planning for node site upgrades, re-homes, or decommission.
- Includes analyzing design requests, interacting with Customer IT Staff to formulate best practice implementations.
- Documenting and presenting alternate network design solutions.
- Provide network As-built documentation including high level design diagram, and network design documents consistent with major design changes to the network
- Provide High, Medium, and Low level design diagrams.
- Track changes and update design documents, as needed, through network duration of contract.
- High Level Network Inventory

**Client Service Manager (CSM)/**

- Monitors Verizon contractual key performance indicators ("KPIs"), service levels, and operating level agreements ("OLAs") as determined with State of West Virginia at engagement planning and kick off;
- Manages the Verizon portfolio of services for change management processes, planning future services demands, and oversight of contract financial compliance between Verizon and State of West Virginia;
- Proactively develops and maintains relationships with executives as well as building new relationships within State of West Virginia;
- Provides management and direction for State of West Virginia and Verizon service and project teams for execution of the Governance Plan as defined below. Conducts reviews to monitor Governance Plan progress and executes remediation as required;

- Reviews your contract performance for compliance with the master agreement terms, including monitoring of all minimum volume commitment thresholds and executing changes as needed. Reports results in the Governance Plan review;
- Develops risk mitigation strategies for customer services as determined with you at engagement planning and kick off;
- Develops solutions for complex business and challenges and provides complex problem solving;
- Provides recommendations during contract negotiations for supportable and executable terms included in this agreement, amendments and SOW's;
- Facilitates communication between State of West Virginia and Verizon executives including escalation and resolution of Verizon or performance issues as required;
- Oversees the initiation and resolution of performance issues requiring escalation and works with State of West Virginia and Verizon technical teams to define overall remediation plans;
- Facilitates beneficial enablement by identifying and executing strategies to increase self-service utilization and expand self-service. Drives online and electronic media tool enablement and adoption;
- Understands your service requirements to facilitate Verizon's integrated solutions ability to meet such requirements;
- Accelerates billing and accounts payable issue resolution by engagement of appropriate State of West Virginia and Verizon resources;
- Financial Management – oversees the identification and resolution of issues negatively affecting State of West Virginia and Verizon financial relationship, such as revenue trends, contractual commitments, accounts payable, etc.;
- SLA Performance Management. Identifies SLAs not being met and liaises with involved departments to execute corrective action. Identification and corrective trends would be represented in a Service Improvement Plan;
- Develops, executes and maintains the Continual Service Improvement Plan;
- Identifies opportunities for service improvement and risk mitigation and engages appropriate State of West Virginia and Verizon resources to execute associated plans;
- Change Management – Identifies and executes improvements in methods, processes and procedures used to institute service and other changes in the overall State of West Virginia/Verizon relationship.

### Client Services Management: Change Manager

- Ensure that standardized methods and procedures are used for all changes
- Provide updates that result from other processes, such as Incident Mgmt. and Configuration Mgmt.
- Review and propose improvements to the change control process
- Obtain Change approval
- Participate in Change Advisory Board (CAB)
- Change reporting

### Financial Service Manager (FSM)

- Supports your billing operations to provide efficient and timely communication;
- Monitors and supports the resolution of all billing related inquiries and the communication with you on progress and conclusion;
- Proactive review of your invoices to pre-empt any billing issues.

### Delivery Manager

- Facilitates implementation and transition pre-planning workshops with Verizon Project Management and partners with Project Managers and Implementation Managers to prepare Implementation Plan.
- Prepares a Business plan for moving from implementation to ongoing operations and maintenance. Manage the transition from implementation to steady state service delivery.
- Coordinates with and works closely with Verizon Project Management to prepare and provide implementation project plans to Verizon personnel and the client Project Managers.
- Provides overall management support for all implementation and deployment activities. Coordinates the solution Implementation with Project Management.
- Establishes communications plan in support of implementation plan with State of West Virginia and Verizon.
- Manages and escalates on any outage and performance issues during implementation to the client, Verizon or third party suppliers, and supports remediation process.

### Project Manager (PM)

- In partnership with the Delivery Manager, responsible for delivering the services agreed at the outset using resources and budget as defined in the Project Initiation Document (PID) and Statement of Works (SOW), aligned with your contracted deliverables;
- Oversees all aspects of project delivery and ensures progress and status is communicated and reviewed in accordance with the business expectations;
- Seeks your approval if any changes are identified in contractual/agreed approaches;
- Partners with Delivery Manager t for all project activities;
- Delivers regular project dashboards and reports to Delivery Manager

## Account Relationship Management

The following is a description of our suggested plan to provide direct, effective contact between State of West Virginia and Verizon:

- Our Executive Management team will meet with your senior executives to discuss our long-term positioning with respect to your key strategic worldwide accounts. Strategic discussions will provide you with insights into potential business strategies and models that may benefit your worldwide businesses;
- On a mutually agreed-upon basis, our Area Vice President will meet with senior-level executives at State of West Virginia to validate the ongoing business relationship between the organizations and evaluate resource requirements and planning;
- Verizon Sales Management will hold quarterly, monthly, or weekly meetings with your management team to manage ongoing initiatives, projects, and resource requirements between the two organizations;
- Executive Visits – State of West Virginia personnel will be invited to attend ongoing executive briefings to discuss new Verizon products and services, determine network goals and strategies, and review the past year's performance;
- Verizon Manager – Service/Program Management and the Service Manager will meet on a mutually agreed upon basis with you to ensure your Service Manager has the authority and resources required to drive the service levels expected by you;
- On a daily basis, the Account Manager will be your point of contact for Verizon and for any of our strategic providers.

## Contact List

### Sales

- 1st Contact: Sandra Hawkins
  Account Manager/Client Partner
  Phone: 304-356-3395
  Email Address: sandra.k.hawkins@verizon.com

- 2nd Contact: Joann Fake
  Sales Manager/Managing Client Partner
  Phone: 717-777-8680
  Email Address: joann.m.fake@verizon.com

- 3rd Contact: Margaret Hallbach
  Area Sales Vice President
  Phone: 703-886-3321
  Email Address: margaret.hallbach@verizon.com

- 4th Contact: Lance Host
  Solutions Architect
  Phone: 304-381-3969
  Email Address: lawrence.host@verizon.com

- 5th Contact: Kin-Fung Chan
  Sr. Manager Solutions Architect
  Phone: 212-652-9558
  Email Address: kin-fung.chan@verizon.com

- 6th Contact: John Donovan Jr
  Managing Director Solutions Architect
  Phone: 919-378-5200
  Email Address: jd.donovan@verizon.com

### Verizon Trouble Resolution

- 1st Contact: Customer Care Center
  800-287-4205

### Service Management Contacts

- Unmanaged – Service Desk – 877-331-4276:
  - 1st Level – Service Desk Personnel – 877-331-4276;
  - 2nd Level – Service Desk Lead – 877-331-4276;
  - 3rd Level – Shemeka Manning – 919-377-3810;

  - 4th Level – Associate Director, Jere Mckinley – 919-377-6113;
  - 5th Level – Director, Kevin Sergent – 919-377-5059.
- Managed Service – MNSO NOC – 800 293-5844 option 1:
  - 1st Level - Assigned Technician – 800-293-5891 option 1;
  - 2nd Level – MNSO Team Lead – 855-896-4911;
  - 3rd Level – Supervisor, William Demery – 919-377-6591;
  - 4th Level – Associate Director, Jere Mckinley – 919-377-6113;
  - 5th Level – Director, Kevin Sergent – 919-377-5059.

### Dedicated Service Manager

- Contact: Lauren Perry
  Service Manager
  Phone: 919-378-3613
  Email Address: lauren.perry@verizon.com
- Contact: Christine Fleming
  Managing Director – Client Services Management
  Phone: 925-951-2687
  Email Address: christine.fleming@verizon.com

We constantly strive to develop new products, enhance our current product offerings, and improve service. The measure of our effectiveness is your satisfaction; therefore, your Verizon Account Team needs your feedback.

Any questions, concerns, or opinions regarding Verizon products or services are welcome. We use this feedback to evaluate and adjust account management activities to improve service to State of West Virginia.

If your comments are product related, your Verizon Account Team can request product modifications or upgrades to better support your requirements.

## Service Level Management

Service Level Management is the process to define the Service Level Agreement (SLA) for State of West Virginia and to monitor service levels to verify contract compliancy. As part of the process, Verizon monitors, measures, and reports on the service performance to verify service level targets are attained.

On a quarterly basis, Verizon will host Service Review meetings with key operational staff and business managers from State of West Virginia and Verizon. The main objective of the Service Review meeting is to:

- Manage the service and operational performance;
- Raise and resolve service lifecycle issues;
- Initiate delivery, SLA and contract changes;
- Monitor the quality of delivery and processes.

During the Service Review meetings, Verizon will present a Governance Dashboard with a series of KPIs against the service level targets. The data is presented on a 12 month rolling basis. The dashboard allows further drill down to a service or geographical location level, to perform detailed analysis and provide historical trending.

## Governance Meetings

It is expected that most issues raised by either party can be resolved at an operational level and regular meetings will be established in order to ensure appropriate alignment between Verizon and State of West Virginia.

For any governance meetings either party may invite additional representatives, if and when required.

The types of meetings are as follows:

| Governance Meeting | Verizon Attendees | Forum Objective | Frequency |
|---|---|---|---|
| Executive Review Meeting | ■ Executive Sponsor;<br>■ Client Partner;<br>■ Sales AVP;<br>■ Director of Service; | Develop long-term value-add strategic global relationship;<br>Review state of relationship, financial, operation and strategic direction; | Annual |
| Contract & Commercial Meeting | ■ Account Director;<br>■ CSM;<br>■ Sales Manager;<br>■ CSM Manager. | Manage on-going commercial relationship between the parties;<br>Continual Service Improvement. | 6 Monthly |
| Service & Operations Meeting | ■ CSM;<br>■ TPM;<br>■ PM. | Review service performance against SLA and provide meaningful improvement recommendations, where appropriate. | Monthly |

| Governance Meeting | Verizon Attendees | Forum Objective | Frequency |
|---|---|---|---|
| Transition Meeting | Delivery Manager and PM team | Review of program, dependencies, issues, risks, and change requirements. | Weekly during the Transition Period. You may request additional meetings on an ad hoc basis as and when required. |

## Risk Management

Verizon will develop a risk mitigation strategy for you, to limit any business disruption and to maintain service quality and performance levels. The Verizon Service Program Manager (CSM) is responsible for identifying and recording the service risks from the outset of the service agreement.

The CSM will apply Risk Management in the following areas:

- Service exposure: analyze each service individually and identify the risks related to the service:
- Contract exposure: review the service agreement between State of West Virginia and Verizon, and identify any contractual, partnership or strategic risks.

If the assessment indicates a number of high levels of risk to the services or the agreement, the Verizon CSM will propose a range of mitigation initiatives to counter these risks.

Verizon will maintain a Risk Register that will be reviewed with you. The Risk Register contains the following details:

- Description of risk;
- Impact of risk on service, cost or quality;
- Likelihood the risk would occur;
- Owner of the risk;
- Risk mitigation initiative.

## Verizon Voice of the Customer Program

The Verizon Voice of the Customer Program is one way to engage State of West Virginia to learn about their experience with Verizon. The program includes:

- Studying the interactions with, and the perceptions from, State of West Virginia at various points thru the customer lifecycle;
- Providing feedback from State of West Virginia to sales leadership, product, service and support organizations regarding the Verizon processes;
- Developing a cohesive action plan to improve the business results and the service experience from State of West Virginia.

Verizon conducts two types of surveys throughout the year.

| | Relationship Survey | Transactional Survey |
|---|---|---|
| Overview | Captures high-level perspectives about the relationship with State of West Virginia and its loyalty to Verizon. | Collects feedback from State of West Virginia following a specific interaction (implementation, repair, etc.) with Verizon. |
| Objective | Provides an indication of State of West Virginia overall satisfaction and loyalty. | Determine potential service gaps and business process improvement initiatives. |
| Frequency | Conducted twice a year. | Ongoing throughout the year. |
| Methodology | Web survey toward specific State of West Virginia respondents;<br>Administered by a leading third-party vendor;<br>Multiple contacts strategy to obtain feedback from decision makers, influencers and key operational staff within the State of West Virginia organization. | |

## Continual Service Improvement

At Verizon, we use Continual Service Improvement in order to learn from past successes and failures. The CSI process implements a closed-loop feedback system as a means to continually improve the effectiveness and efficiency of services and processes.

To ensure any improvements are embedded, we use the survey results to document a Continual Service Improvement Plan achieving a higher quality of service by developing and implementing service management processes and continual re-evaluation.

## Customer Care

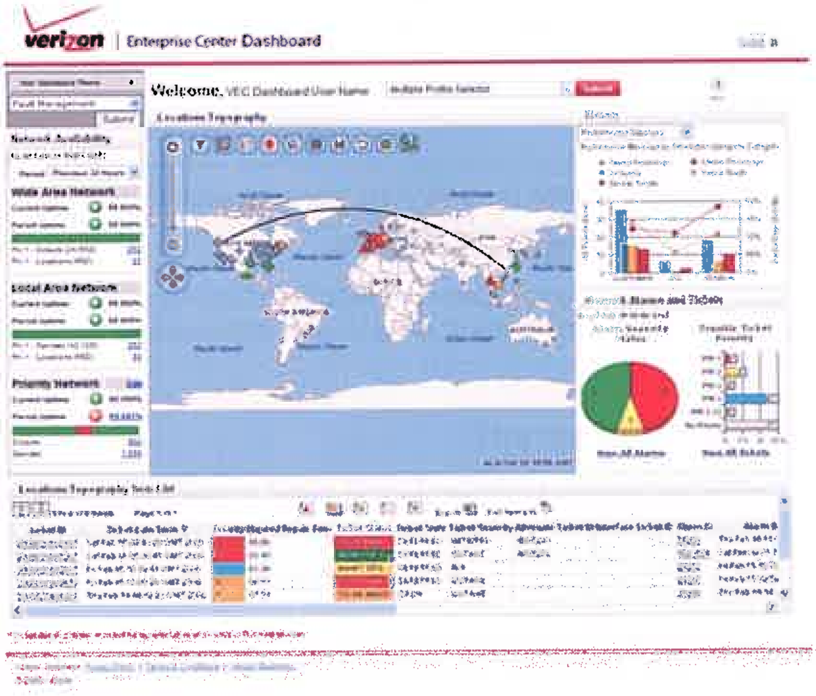
At Verizon, we have a process to manage standardized non-technical Billing Inquiries, different from Service Incidents which are handled thru the Incident Management process.

In addition to the Billing Program Manager we can address the Billing Inquiries from State of West Virginia with standardized and automated procedures. Billing Inquiries can be raised by State of West Virginia thru the Verizon Enterprise Center portal. For guidance on how to open an inquiry please visit the online demo https://www.verizonenterprise.com/us/Support/billing/

Once the Billing Inquiry is raised, State of West Virginia will receive an auto-response advising of the Inquiry number. The Customer Care Team will then work on resolving your inquiry.

If you are not a Verizon Enterprise Center user, to raise a non-technical Billing Inquiry, send an email to the relevant address below.

| Country | Email Address |
|---|---|
| U.S. | customercare@verizon.com |



*Verizon Enterprise Center Dashboard*

The complete Verizon Enterprise Center Overview per region, including the different Verizon Enterprise Center User and Reference guides, are available on the Verizon Commercial Training site at https://customertraining.verizon.com. If you need assistance please contact us at 1-800-264-1000.

We seek to create the connections that advance global businesses and enrich lives. We're passionate about technologies that enable people to focus on their strengths, to bring their talents to the market, to create freely, and to connect with others without fear of hindrance. We drive technology forward.

Please refer to our attached icon(s) below, pertaining to Project, Order, and Billing/Services Management. For hardcopy purposes, please review the following page(s).

Project Management Overview State of W

Service Program Management slides.p

Verizon_Enterprise_Solutions_S rev 4_021

# We deliver the connected world. Simply. Reliably. Securely.

**Better experiences.**

**Better business results.**

**Better peace of mind.**

Simple

Global

Secure

Value

Reliable

Managed

**Technology partner attributes**

# Speed and quality: what it takes.

### Simple structure

- Easy to navigate
- Clear ownership

### Common platform

- Built for scale
- Easy to integrate

### Efficient processes

- Accountability
- Accuracy / quality

### Quality metrics

- Voice of customer
- Deliver the promise

### Innovation

- Iteration
- Crowdsourcing

# Project Management

## Customer Challenges

- Maintain Business Growth
- Cost Containment
- On-time Delivery of Projects
- Limited Resources
- Rapid Transition to New Technology
- Vendor Satisfaction
- Manage Risk and Reliability

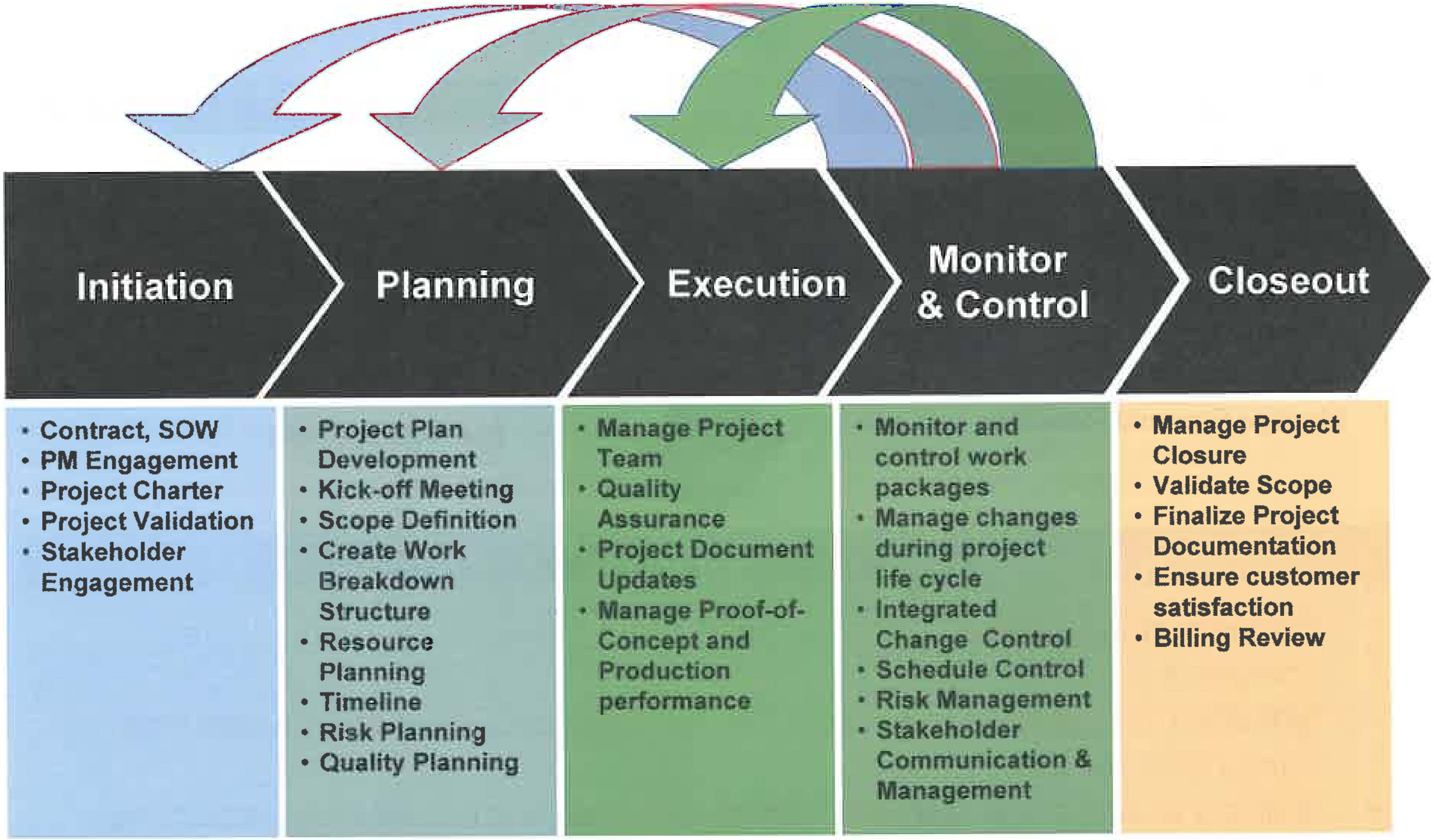
## Project Management Capabilities

- Scope Management
- Project Governance
- Schedule Management
- Human Resources Management
- Solution Management
- Quality Management
- Risk Management

## Proven Expertise

- **Delivery management** for enterprise client networks of various levels complexity
- **Solution integration** in network, technology, and application areas that bring clients value
- Built on widely accepted **PMI framework** used across multiple industries

# Project Management Process Groups



**Initiation**

- Contract, SOW
- PM Engagement
- Project Charter
- Project Validation
- Stakeholder Engagement

**Planning**

- Project Plan Development
- Kick-off Meeting
- Scope Definition
- Create Work Breakdown Structure
- Resource Planning
- Timeline
- Risk Planning
- Quality Planning

**Execution**

- Manage Project Team
- Quality Assurance
- Project Document Updates
- Manage Proof-of-Concept and Production performance

**Monitor & Control**

- Monitor and control work packages
- Manage changes during project life cycle
- Integrated Change Control
- Schedule Control
- Risk Management
- Stakeholder Communication & Management

**Closeout**

- Manage Project Closure
- Validate Scope
- Finalize Project Documentation
- Ensure customer satisfaction
- Billing Review

# Project Management Value

- ✓ Customer requirements are clearly defined, understood, and accepted among all stakeholders
- ✓ Critical project activities are identified, scheduled, monitored, and controlled, including continued alignment to project objectives
- ✓ Customers and other constituents are kept up-to-date with full visibility of project status
- ✓ Project risks are identified, monitored, and mitigated during the project life cycle
- ✓ The quality of project deliverables is controlled and monitored to meet the project objectives
- ✓ Sufficient resources and attention are given to meet the project timeline

# Project Management Enterprise Benefits

*Experienced*

- VES has over 20 years of experience providing project management on varying scales and complexity to enterprise customers world wide, and to the state, local, and U.S. Federal Government

*Meaningful*

- VES delivers project management in the global networking technology and applications areas that customers need most, and where they are less likely to have the desire or expertise to perform services themselves

*Qualified*

- VES Project Management is an extension of Verizon's Professional Services built on the Project Management Institute's (PMI) best practice framework, providing customers expertise and complete solutions based on their unique needs

*Skilled*

- VES offers expertise at key stages throughout the project lifecycle, ensuring continuity from planning to implementation enabling end-to-end complete solutions

# Project Management Customer Testimonies

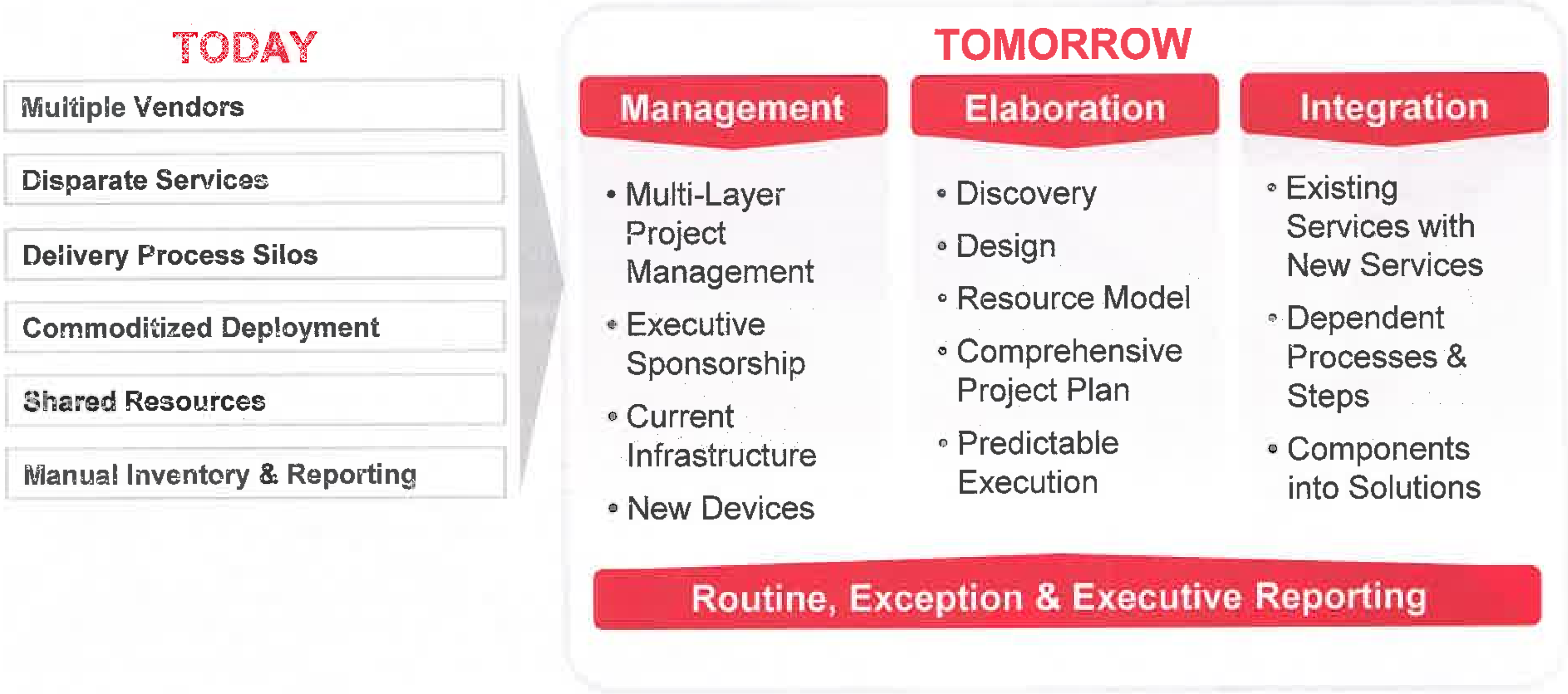
"Excellent synergy and collaboration with the whole Verizon Team starting from the Project Manager all the way down [to the] technicians. Project well done."

"This has been a multi year project that has seen its up and downs from vendors and customer perspective. **The one steady and reliable role of the project has been the Project Manager.** She has always presented herself as a professional and has gone above and beyond to keep all parties up-to-date on status and pending items. Due to her commitment and passion around her role we have been able to…move forward with reliable information and next steps."

"Jody is a tremendous project manager. **Always organized and takes command of the calls/project.** Highly recommend Jody for any future project."

"The Verizon team supporting [the project] were outstanding. Very professional and focused on quality in delivery. Ann (PM) performed a key role in the success of delivery and issue resolution. She has tremendous experience and works well with every team member, regardless of level or company. There were multiple Telco vendors involved and the Verizon team raised expectations for all. **The…program would not have been successful with out a true partnership with Verizon.** Great work!."

# Project Management Transition Migration



## TODAY

- Multiple Vendors
- Disparate Services
- Delivery Process Silos
- Commoditized Deployment
- Shared Resources
- Manual Inventory & Reporting

## TOMORROW

### Management

- Multi-Layer Project Management
- Executive Sponsorship
- Current Infrastructure
- New Devices

### Elaboration

- Discovery
- Design
- Resource Model
- Comprehensive Project Plan
- Predictable Execution

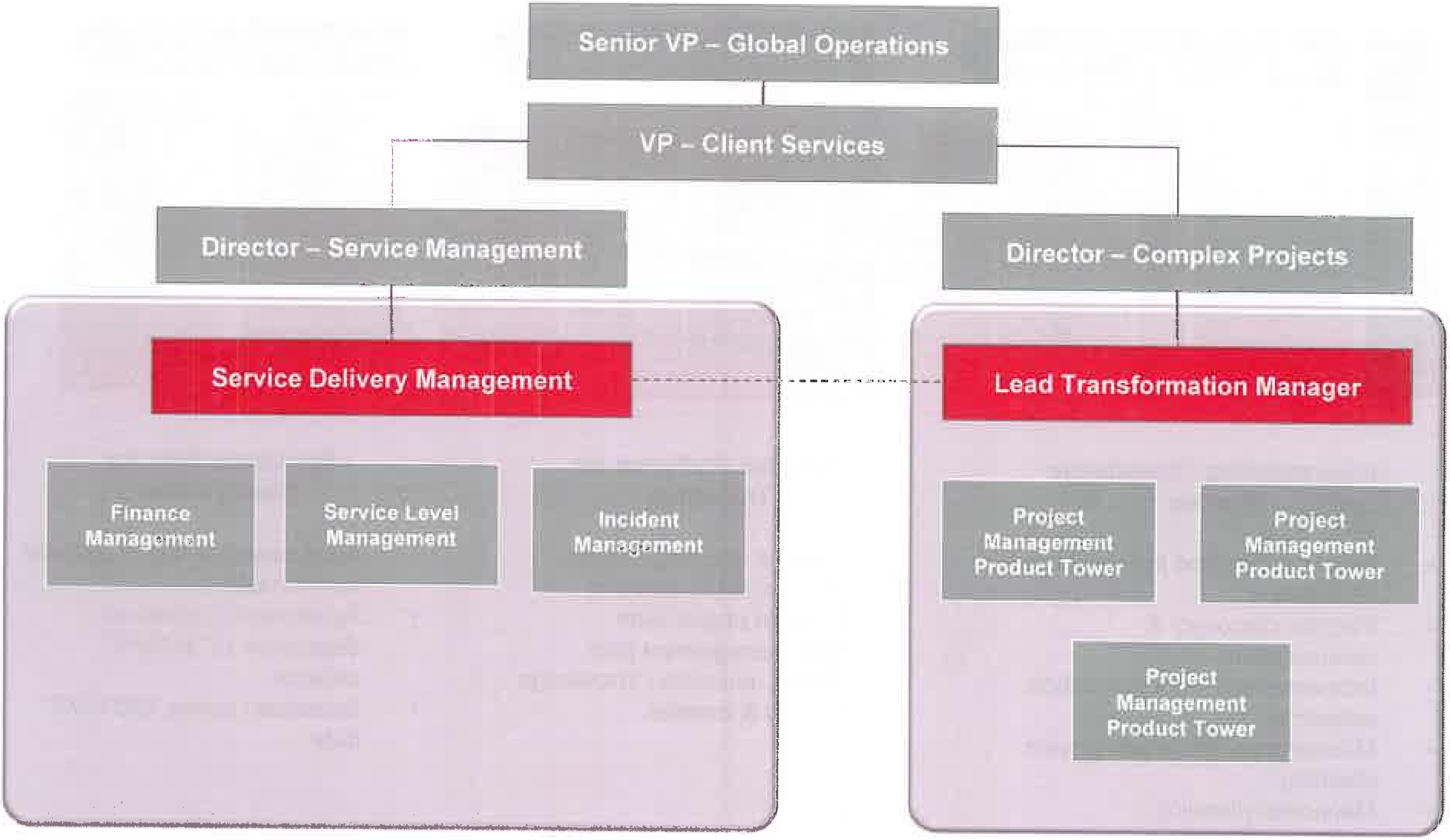
### Integration

- Existing Services with New Services
- Dependent Processes & Steps
- Components into Solutions

**Routine, Exception & Executive Reporting**

***Shift to an All-Inclusive Approach to Transition Services***

# Project Management Transformation Service Structure Example



Senior VP – Global Operations

VP – Client Services

Director – Service Management

Director – Complex Projects

Service Delivery Management

Finance Management

Service Level Management

Incident Management

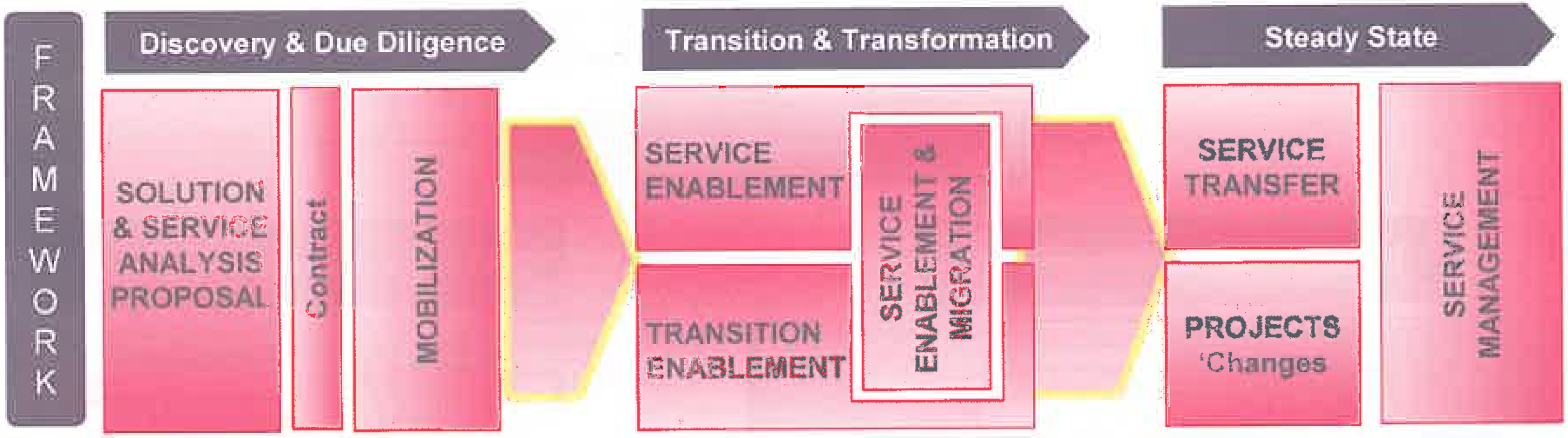
Lead Transformation Manager

Project Management Product Tower

Project Management Product Tower

Project Management Product Tower

# Project Management High Level Transition Approach



FRAMEWORK

Discovery & Due Diligence

SOLUTION & SERVICE ANALYSIS PROPOSAL

Contract

MOBILIZATION

Transition & Transformation

SERVICE ENABLEMENT

TRANSITION ENABLEMENT

SERVICE ENABLEMENT & MIGRATION

Steady State

SERVICE TRANSFER

PROJECTS 'Changes

SERVICE MANAGEMENT

**Understanding / Knowledge Sharing**

- Initial solution and proposal level of diligence
- Portfolio discovery & reconciliation
- Interviews and work instruction collection
- Milestone schedule and project planning
- Manpower planning

**Build the Platforms for Transition**

- Process mapping, inputs / outputs, RACI matrices
- Detailed project plan
- Risk management plan
- Create runbooks / knowledge sharing & transfer

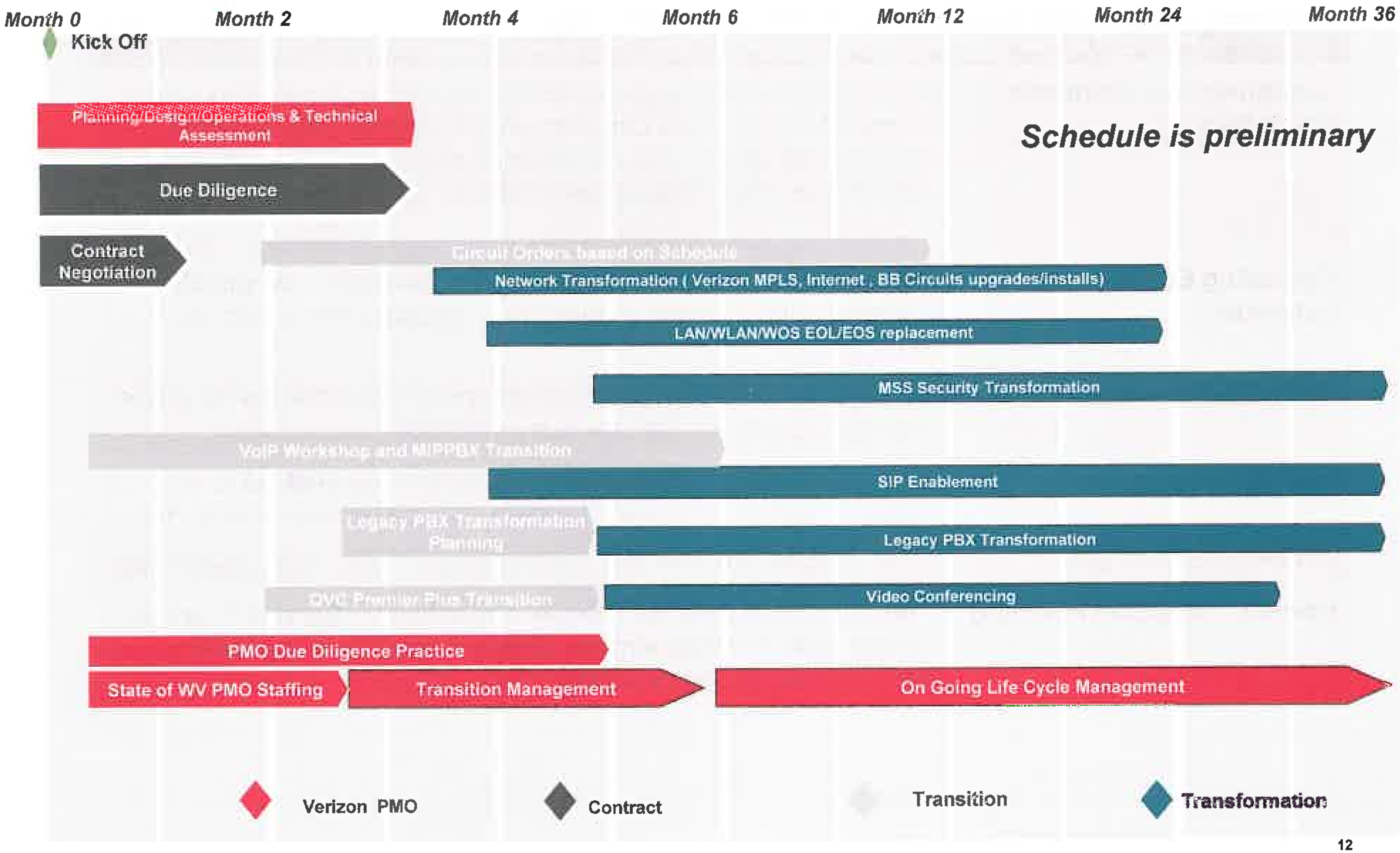
**Readiness Gate for Steady State**

- Acceptance testing of process functionality
- Agreement reached on disposition of “in-flight” projects
- Schedule / agree “GO LIVE” date

# Project Management Due Diligence Phase

| Reasons for conducting a comprehensive Due Diligence Phase: | |
|---|---|
| **Customer Requirements Validation** | Identify, verify, and align expectations to ensure the proposed scope of the services complies with customer requirements Analyze the operational implications and financial ramifications of potential contract-based relationships |
| **Operating Environment Validation** | Validate current Service Operating Environments for supplier capability and integration planning in preparation to migrate support |
| **Third-Party Validation** | Qualify any Third-Party service responsibilities that are in-scope and may require further service integration preparation |
| **Risk Mitigation** | Identify, validate, and mitigate joint contractual **Risk(s)** to all stakeholders, and reduce on-going financial and operating risk |
| **Assumption Validation** | Drive toward **“zero-based”** Assumptions Award and delivery plan |
| **Service Transition Planning** | Prepare and provide for a timely and effective **Service Transition** for the State of West Virginia. Enhance customer transition performance and satisfaction. |

# Project Management Transition & Transformation Example Schedule



Month 0

Month 2

Month 4

Month 6

Month 12

Month 24

Month 36

Kick Off

*Schedule is preliminary*

Planning/Design/Operations & Technical Assessment

Due Diligence

Contract Negotiation

Circuit Orders based on Schedule

Network Transformation ( Verizon MPLS, Internet , BB Circuits upgrades/installs)

LAN/WLAN/WOS EOL/EOS replacement

MSS Security Transformation

VoIP Workshop and MIPPBX Transition

SIP Enablement

Legacy PBX Transformation Planning

Legacy PBX Transformation

DVC Premier Plus Transition

Video Conferencing

PMO Due Diligence Practice

State of WV PMO Staffing

Transition Management

On Going Life Cycle Management

Verizon PMO

Contract

Transition

Transformation

# Service Program Management Enterprise Benefits

*Experienced*

- VES has over 20 years of experience providing Service Management on varying scales and complexity to enterprise customers world wide, and to the state, local, and U.S. Federal Government

*Qualified*

- VES provides Service Program Managers with knowledge and expertise in State and Local Government customer networks and Verizon services and products. Continuous training and certifications are a Verizon requirement.

*Dedication to the State*

- VES Service Program Management is dedicated to the State of WV and partners with the State of WV on service, billing, Verizon portal engagement and other support services.

verizon✓

Confidential and proprietary materials for authorized Verizon personnel and outside agencies only. Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement.

# Service Program Management For State of WV

**Billing**

- Supports your billing operations to provide efficient and timely communication
- Monitors and supports resolution of all billing related inquiries
- Provides billing reports as required
- Meet on an as needed basis to resolve disputes in a timely manner to keep charges, payments, credits as current as possible.
- Participate in order status meetings to ensure billing matches the service
- Assist in accessing invoices and reports through the Verizon portal

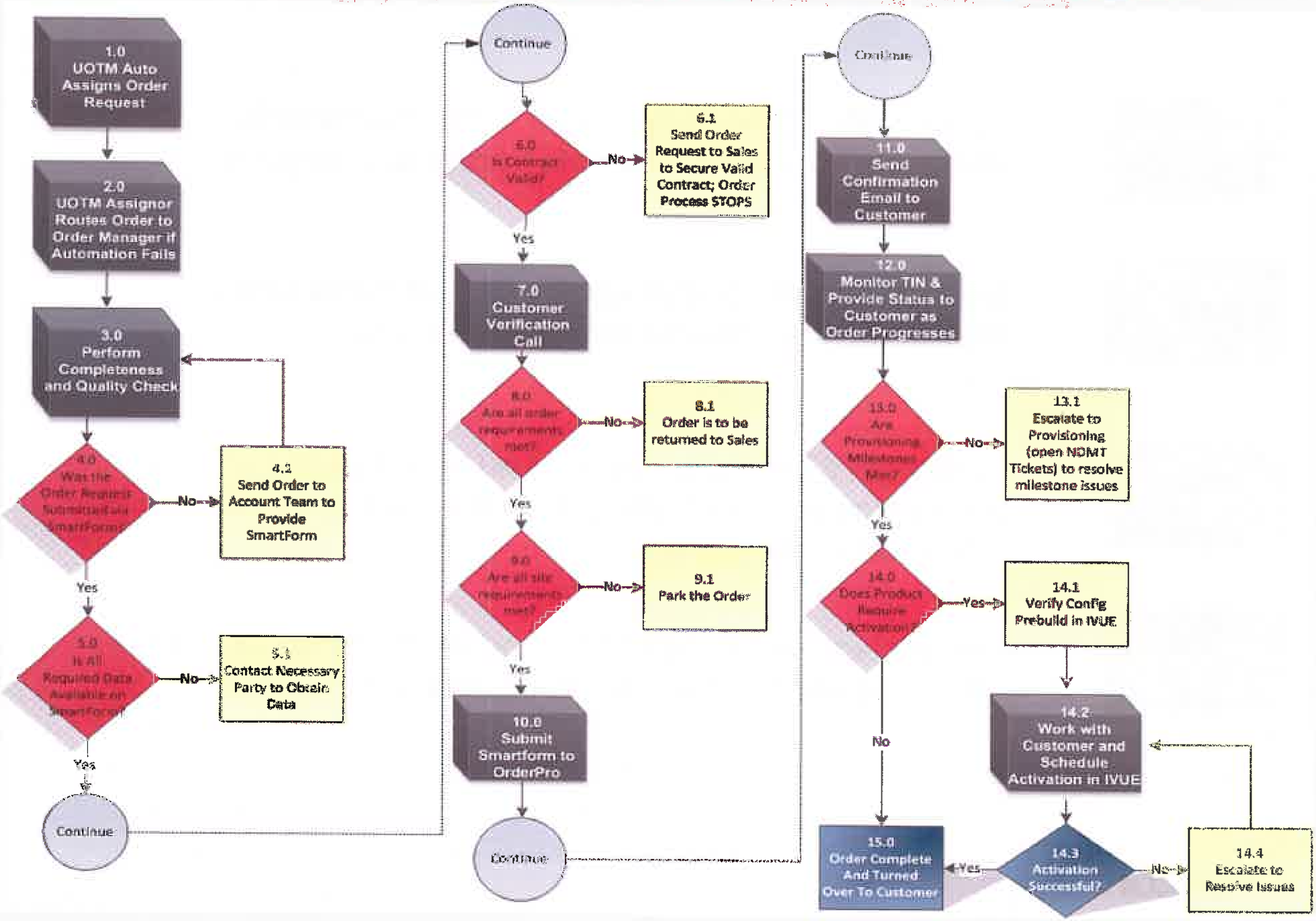
# Service Program Management For State of WV

Service

- Monitors, measures, and reports on service performance
- Host service and governance review meetings to identify and resolve any service and or process issues
- Manages individual complex technical incidents and problems impacting service availability and escalate as appropriate
- Manages conference bridges as necessary and manages action plan to restore service
- Reviews the performance of the network/network optimization
- Interfaces with Verizon support centers and third party carrier centers as required
- Provides Verizon portal support to State of WV
- Identifies opportunities for service improvement.  Provides root cause analysis reports as needed.

Confidential and proprietary materials for authorized Verizon personnel and outside agencies only  Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement

# Government/Education Order Manager Procedure



1.0
UOTM Auto Assigns Order Request

2.0
UOTM Assignor Routes Order to Order Manager if Automation Fails

3.0
Perform Completeness and Quality Check

4.0
Was the Order Request Submitted on a SmartForm?

No

4.1
Send Order to Account Team to Provide SmartForm

Yes

5.0
Is All Required Data Available on SmartForm?

No

5.1
Contact Necessary Party to Obtain Data

Yes

Continue

Continue

6.0
Is Contract Valid?

No

6.1
Send Order Request to Sales to Secure Valid Contract; Order Process STOPS

Yes

7.0
Customer Verification Call

8.0
Are all order requirements met?

No

8.1
Order is to be returned to Sales

Yes

9.0
Are all site requirements met?

No

9.1
Park the Order

Yes

10.0
Submit Smartform to OrderPro

Continue

Continue

11.0
Send Confirmation Email to Customer

12.0
Monitor TIN & Provide Status to Customer as Order Progresses

13.0
Are Provisioning Milestones Met?

No

13.1
Escalate to Provisioning (open NDMT Tickets) to resolve milestone issues

Yes

14.0
Does Product Require Activation?

Yes

14.1
Verify Config Prebuild in IVUE

14.2
Work with Customer and Schedule Activation in IVUE

14.3
Activation Successful?

No

14.4
Escalate to Resolve Issues

Yes

No

15.0
Order Complete And Turned Over To Customer

# Order Management - Benefit to State of WV

**Assigned Order Manager**

State of WV will be assigned an Order Manager that will handle your order requests from cradle to grave.

**Timely Status Update**

State of WV will receive weekly spreadsheets upon their request and hold weekly calls as well.

**Experienced Installation**

State of WV orders will be tracked from Sales submission through order entry, provisioning, Install and activation if that applies.

**Dedication to the State**

The account will be hand held and whatever is needed will be provided to them on an individual case basis.

# Attachment A. Cost Sheet

Please reference the separate Cost Proposal provided by Verizon as requested.

# Attachment B. HIPAA – BAA

Please refer to our attached icon(s) below, pertaining to HIPAA – BAA. For hardcopy purposes, please review the following page(s).

Attachment B
(BAA)--(WV RFP) Veri

**ATTACHMENT B**

**WV STATE GOVRNMENT**
**HIPAA BUSINESS ASSOCIATE ADDENDUM**

**Verizon Proposed Modifications**

**3. Obligations of Associate.**

**l. Notification of Breach.** During the term of this Addendum, the Associate shall notify the Agency and, unless otherwise directed by the Agency in writing, the WV Office of Technology **within 24 hours** ~~immediately~~by e-mail or web form upon the discovery of any Breach of unsecured PHI**. The Associate shall report on a periodic basis.**~~; or within 24 hours~~ by e-mail or web form~~,~~ ~~of~~any suspected Security Incident, intrusion or unauthorized use or disclosure of PHI in violation of this Agreement and this Addendum, or potential loss of confidential data affecting this Agreement. Notification shall be provided to the Agency Procurement Officer at www.state.wv.us/admin/purchase/vrc/agencyli.htm and, unless otherwise directed by the Agency in writing, the Office of Technology at incident@wv.gov or https://apps.wv.gov/ot/ir/Default.aspx.

The Associate shall immediately investigate such Security Incident, Breach, or unauthorized use or disclosure of PHI or confidential data. Within 72 hours of the discovery **(with respect to a Breach of unsecured PHI) or within 72 hours of providing notice of a suspected Security Incident, intrusion or unauthorized use or disclosure of PHI, or potential loss of confidential data**, the Associate shall notify the Agency Procurement Officer, and, unless otherwise directed by the Agency in writing, the Office of Technology of: (a) Date of discovery; (b) What data elements were involved and the extent of the data involved in the Breach; (c) A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed PHI or confidential data; (d) A description of where the PHI or confidential data is believed to have been improperly transmitted , sent, or utilized; (e) A description of the probable causes of the improper use or disclosure; and (f) Whether any federal or state laws requiring individual notifications of Breaches are triggered.

Agency will coordinate with Associate to determine additional specific actions that will be required of the Associate for mitigation of the Breach, which may include notification to the individual or other authorities.

~~All associated costs shall be borne by the Associate. This may include, but not be limited to costs associated with notifying affected individuals.~~

If the Associate enters into a subcontract relating to the Agreement where the subcontractor or agent receives PHI as described in section 2.a. of this Addendum, all such subcontracts or downstream agreements shall contain the same incident notification requirements as contained herein, with reporting directly to the Agency Procurement Officer. Failure to include such requirement in any subcontract or agreement may result in the Agency's termination of the Agreement.

**m. Assistance in Litigation or Administrative Proceedings.** The Associate shall **use commercially reasonable efforts to** make itself and any subcontractors, workforce or agents assisting Associate in the performance of its obligations under this Agreement, available to the Agency at no cost to the Agency to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against the Agency, its officers or employees based upon claimed violations of HIPAA, the HIPAA regulations or other laws relating to security and privacy, which involves inaction or actions by the Associate, except where Associate or its subcontractor, workforce or agent is a named as an adverse party.

# Attachment C. Telecommunications Change Request

Attachment_C
Telecommunications

## Verizon Response

Verizon has read and understands.

ATTACHMENT_C

## STATE OF WEST VIRGINIA - VOIP TELECOMMUNICATIONS CHANGE REQUEST (TCR)

**NOTE: FIELDS WITH ** ARE COMPLETED BY WVOT**

### AGENCY TCR INFORMATION

| | | | |
|---|---|---|---|
| TCR#** | | REQUESTED DUE DATE | |
| AGENCY DEPARTMENT | | AGENCY NAME | |
| DIVISION | | DIRECT BILL** | NO |
| AGENCY PRIMARY CONTACT | | AGENCY ON-SITE CONTACT | |
| AGENCY PRIMARY CONTACT PHONE | | AGENCY ON-SITE CONTACT PHONE | |
| AGENCY PRIMARY CONTACT EMAIL | | AGENCY ON-SITE CONTACT EMAIL | |
| OFFICE HOURS OF OPERATION | | OFFICE MOVE | |
| AGENCY ON-SITE ADDRESS (E911) | | OLD ADDRESS (IF APPLICABLE) | |
| | | | |
| WVOT FIELD TECH(S)** | | WVOT FIELD TECH(S) PHONE** | |

### REQUESTED VOIP SERVICE(S) Account numbers located on Telecommunications Backup

| | | | |
|---|---|---|---|
| VOIP ACCOUNT NUMBER | | | |
| Requested Services- Mark Yes for all that apply | | | |
| Hosted VOIP-New Implementation | | Hosted Virtual Contact Center-New Implementation | |
| Hosted VOIP- Existing -Add | | Hosted Virtual Contact Center-Existing-Add | |
| Hosted VOIP- Existing -Move | | Hosted Virtual Contact Center-Existing-Move | |
| Hosted VOIP- Existing -Change | | Hosted Virtual Contact Center-Existing-Change | |
| Hosted VOIP- Existing -Delete | | Hosted Virtual Contact Center-Existing-Delete | |
| IP Contact Center Services | | WebEx | |
| Open Video Communications | | Audio Conferencing | |
| Other | | | |
| COMMENTS-Details | | | |

### AGENCY AUTHORIZATION- PLEASE PRINT NAMES AND THEN SIGN OR RETURN AUTHORIZATION VIA EMAIL

| | | |
|---|---|---|
| AGENCY AUTHORIZATION | x<br>AGENCY AUTHORIZATION (PRINTED) | x<br>AGENCY AUTHORIZATION(SIGNATURE) |
| COMPLETED BY | x<br>COMPLETED BY (PRINTED) | x<br>COMPLETED BY (SIGNATURE) |

*PLEASE SIGN ABOVE AND RETURN TO TCR@WV.GOV TCR MAY BE REJECTED IF REQURIED FIELDS ARE INCOMPLETE*

| | | |
|---|---|---|
| WVOT AUTHORIZATION | x<br>WVOT AUTHORIZATION (COMPLETED BY WVOT) | x<br>RECEIVED BY/DATE (COMPLETED BY WVOT) |

## STATE OF WEST VIRGINIA - VOIP TELECOMMUNICATIONS CHANGE REQUEST (TCR)

**NOTE: FIELDS WITH ** ARE COMPLETED BY WVOT**

### AGENCY TCR INFORMATION

| | | | |
|---|---|---|---|
| TCR#** | | REQUESTED DUE DATE | |
| AGENCY DEPARTMENT | | AGENCY NAME | |
| DIVISION | | | |
| Full Street Address (911) | | | |
| Number of Users | | Is the location VOIP Ready? | |
| Number of auto attendants by location | | Do you plan to use Device Mobility? | |
| Do any locations require a phased install? | | | |
| Will any users use soft phones only? | | If so, how many? | |
| Do you plan to use Extension Mobility? | | If so, how many phones? | |
| Number of Hunt Groups | | | |
| Are any members of the hunt group off net? | | If so, how many? | |
| Do you plan use SRST at each site in case of loss of connectivity to the UCCaas data centers? | | If so, please describe the connectivity for each location: | |
| | | Quantity | |
| | | Type of Calls Allowed | |
| | | Any other details. | |

# West Virginia Office of Technology

## Instructions for Completing a Telecommunications Change Request (TCR)

Note: Fields with ** are Completed by WVOT

These instructions are to be followed when submitting TCRs to add, change, or disconnect voice and/or data services obtained through the statewide contracts. If ordering both voice$IP, and data services, separate TCRs will be needed for each type of service. If ordering service to be billed to more than one billing account, separate TCRs will be needed for each billing account.

All TCRs must be typed in order to ensure accurate service delivery. Only complete TCR forms can be processed. The Telecommunications Ordering and Billing section can assist with the completion of the TCR and any questions regarding required fields by emailing TCR@wv.gov. Please allow time for technical and business consultations and research when necessary.

The date of submission is the date that a complete TCR is provided to the vendor. Timeframes associated with the installation of services requested begin when a complete TCR is submitted to the vendor. Timeframes to be associated with the installation and/or disconnection of services are governed by the particular statewide contract(s) and/or Service Level Agreement(s) for each specific service; however, if the vendor requires special construction, then the contract timelines are not in effect. Please consult WVOT with questions.

Email the completed TCR and any related correspondence to TCR@wv.gov. Do not send a TCR and related correspondence to an individual email address as this could cause delays.

### Information Requested on a TCR:

| AGENCY INFORMATION | DESCRIPTION OF INFORMATION REQUESTED |
|---|---|
| TCR# ** | This is the number that must be referenced when requesting the status of any TCR. |
| Requested Due Date | "ASAP" cannot be accepted. Due dates are subject to vendor requirements. |
| Agency Department (REQUIRED) | Use Department [Org Level 1] (i.e. Transportation) |
| Agency Name (REQUIRED) | Use Agency Name [Org Level 2] (i.e. Division of Highways) |
| Division | Use Division name [Org Level 3], when applicable (i.e. Highways District 1) |
| Direct Bill? | This is always "No" unless a waiver to go off the State Wide Contract is provided by OT. |
| Agency Primary Contact (REQUIRED) | This is the decision maker who should be contacted if there are questions regarding TCR costs and/or due date. |
| Agency Primary Contact Phone # (REQUIRED) | Agency Primary Contact's phone number including extension, if applicable. |
| Agency Primary Contact Email (REQUIRED) | Agency Primary Contact's email address. |
| Office Hours of Operation | The hours the office is open for an on-site visit if it is necessary to review, design and/or install the requested services. |
| Agency On-site Contact (REQUIRED) | This person should be on-site and available to provide access to location and have knowledge of the work request. |
| Agency On-site Contact Phone# (REQUIRED) | Agency On-site Contact's phone number including extension, if applicable. |
| Agency On-site Contac Email (REQUIRED) | Agency On-site Contact's email address |
| Agency On-site Address (REQUIRED) | The E911 physical address of the location, including the zip code and county, where the requested services are to be performed. |
| Office Move? (REQUIRED) | If the request is associated with an office move, select "Yes." |
| Old Address (if applicable) | If Office Move is marked as "Yes", enter the E911 physical address of the location the services are moving from. |
| WVOT Field Tech ** | WVOT Field Technician assigned to assist with installation details. |
| Phone ** | WVOT Field Tech's phone number. |
| Email ** | WVOT Field Tech's email address. |
| REQUESTED VOIP SERVICES | DESCRIPTION OF INFORMATION REQUESTED |
| VOIP Account Number | This is the 6 digit account number that is available on the billing backup. It is also the agency's main ID number. |
| Requested Services-Mark Yes For All That Apply | |
| Hosted VOIP-New Implementation | If this request is to add a new Hosted VOIP Implementation, select "Yes" |
| Hosted VOIP- Existing -Add | If this request is to add services for an existing Hosted VOIP Implementation, select "Yes" |
| Hosted VOIP- Existing -Move | If this request is to move services for an existing Hosted VOIP Implementation, select "Yes" |
| Hosted VOIP- Existing -Change | If this request is to change services for an existing Hosted VOIP Implementation, select "Yes" |
| Hosted VOIP- Existing -Delete | If this request is to delete services for an existing Hosted VOIP Implementation, select "Yes" |
| IP Contact Center Services | If this request is to add services for an IP Contact Center Service, select "Yes" |
| Open Video Communications | If this request is to add services for an Open Video Communications, select "Yes" |
| Hosted Virtual Contact Center-New Implementation | If this request is to add a new Hosted Virtual Contact Center, select "Yes" |
| Hosted Virtual Contact Center-Existing-Add | If this request is to add services for an existing Hosted Virtual Contact Center, select "Yes" |
| Hosted Virtual Contact Center-Existing-Move | If this request is to move services for an existing Hosted Virtual Contact Center, select "Yes" |
| Hosted Virtual Contact Center-Existing-Change | If this request is to change services for an existing Hosted Virtual Contact Center, select "Yes" |
| Hosted Virtual Contact Center-Existing-Delete | If this request is to delete services for an existing Hosted Virtual Contact Center, select "Yes" |
| WebEx | If this request is to add services for an WebEx, select "Yes" |
| Audio Conferencing | If this request is to add services for an Audio Conferencing, select "Yes" |
| Comments | Use the comments section to provide requested service summary and additional explanation of the service(s) requested. If this is an emergency, "EXPEDITE" will be written in this section. Additional charges may apply for expedite requests. |

| AGENCY AUTHORIZATION | DESCRIPTION OF INFORMATION REQUESTED |
|---|---|
| Agency Authorization | This is the person (name both printed and signed) designated by the agency as having authorization to submit TCRs for voice and/or data related services on behalf of the agency. This person should have financial authorization since a TCR obligates an agency to financial responsibility of the requested services. The WVOT is obligated to accept TCRs for services from any employee within that agency and the agency will be responsible for any charges resulting from the services requested on the TCR. The agency needs to complete a Signature Authority Designation form for all individuals authorized to sign TCRs and submit updated designation forms to the Telecommunications Ordering and Billing section (TCR@wv.gov). |
| Completed by | This is the individual (name both printed and signed) who completed the TCR form. |
| WVOT Authorization ** | This is the individual within WVOT who authorizes the TCR be submitted to the vendor. |
| Received by / Date ** | This is the individual within WVOT who received the TCR from the agency and the date the TCR was received by WVOT. |

# Attachment D. Purchasing Affidavit

Please reference the Purchasing Affidavit provide on the following page(s).

STATE OF WEST VIRGINIA
Purchasing Division

# PURCHASING AFFIDAVIT

**CONSTRUCTION CONTRACTS:** Under W. Va. Code § 5-22-1(i), the contracting public entity shall not award a construction contract to any bidder that is known to be in default on any monetary obligation owed to the state or a political subdivision of the state, including, but not limited to, obligations related to payroll taxes, property taxes, sales and use taxes, fire service fees, or other fines or fees.

**ALL CONTRACTS:** Under W. Va. Code §5A-3-10a, no contract or renewal of any contract may be awarded by the state or any of its political subdivisions to any vendor or prospective vendor when the vendor or prospective vendor or a related party to the vendor or prospective vendor is a debtor and: (1) the debt owed is an amount greater than one thousand dollars in the aggregate; or (2) the debtor is in employer default.

**EXCEPTION:** The prohibition listed above does not apply where a vendor has contested any tax administered pursuant to chapter eleven of the W. Va. Code, workers' compensation premium, permit fee or environmental fee or assessment and the matter has not become final or where the vendor has entered into a payment plan or agreement and the vendor is not in default of any of the provisions of such plan or agreement.

**DEFINITIONS:**

**"Debt"** means any assessment, premium, penalty, fine, tax or other amount of money owed to the state or any of its political subdivisions because of a judgment, fine, permit violation, license assessment, defaulted workers' compensation premium, penalty or other assessment presently delinquent or due and required to be paid to the state or any of its political subdivisions, including any interest or additional penalties accrued thereon.

**"Employer default"** means having an outstanding balance or liability to the old fund or to the uninsured employers' fund or being in policy default, as defined in W. Va. Code § 23-2c-2, failure to maintain mandatory workers' compensation coverage, or failure to fully meet its obligations as a workers' compensation self-insured employer. An employer is not in employer default if it has entered into a repayment agreement with the Insurance Commissioner and remains in compliance with the obligations under the repayment agreement.

**"Related party"** means a party, whether an individual, corporation, partnership, association, limited liability company or any other form or business association or other entity whatsoever, related to any vendor by blood, marriage, ownership or contract through which the party has a relationship of ownership or other interest with the vendor so that the party will actually or by effect receive or control a portion of the benefit, profit or other consideration from performance of a vendor contract with the party receiving an amount that meets or exceed five percent of the total contract amount.

**AFFIRMATION: By signing this form, the vendor's authorized signer affirms and acknowledges under penalty of law for false swearing (*W. Va. Code* §61-5-3) that: (1) for construction contracts, the vendor is not in default on any monetary obligation owed to the state or a political subdivision of the state, and (2) for all other contracts, that neither vendor nor any related party owe a debt as defined above and that neither vendor nor any related party are in employer default as defined above, unless the debt or employer default is permitted under the exception above.**

**WITNESS THE FOLLOWING SIGNATURE:**

Vendor's Name: Verizon Business Network Services Inc. on behalf of MCI Communications Services, Inc. dba Verizon Business Services

Authorized Signature: ______________________ Date: November 20, 2018

State of Oklahoma

County of Tulsa, to-wit:

Taken, subscribed, and sworn to before me this 20 day of November, 2018.

My Commission expires 03-01, 2020

**AFFIX SEAL HERE** **NOTARY PUBLIC** Brandy

BRANDY FITZLOFF
NOTARY PUBLIC-STATE OF OKLAHOMA
COMMISSION # 12002043
MY COMMISSION EXPIRES 03-01-2020

# Attachment E. Disclosure of Interested Parties to Contracts

Attachment E
Ethics_DisclosureInt

## Verizon Response

Verizon believes the Disclosure of Interested Parties to Contract is not applicable since MCI Communications Services, Inc. d/b/a Verizon Business Services is a wholly owned indirect subsidiary of Verizon Communications Inc. which is a publicly traded entity.

West Virginia Ethics Commission

# Disclosure of Interested Parties to Contracts

Pursuant to *W. Va. Code* § 6D-1-2, a state agency may not enter into a contract, or a series of related contracts, that has/have an actual or estimated value of $1 million or more until the business entity submits to the contracting state agency a Disclosure of Interested Parties to the applicable contract. In addition, the business entity awarded a contract is obligated to submit a supplemental Disclosure of Interested Parties reflecting any new or differing interested parties to the contract within 30 days following the completion or termination of the applicable contract.

For purposes of complying with these requirements, the following definitions apply:

*"Business entity"* means any entity recognized by law through which business is conducted, including a sole proprietorship, partnership or corporation, but does not include publicly traded companies listed on a national or international stock exchange.

*"Interested party"* or *"Interested parties"* means:

(1) A business entity performing work or service pursuant to, or in furtherance of, the applicable contract, including specifically sub-contractors;
(2) the person(s) who have an ownership interest equal to or greater than 25% in the business entity performing work or service pursuant to, or in furtherance of, the applicable contract. (This subdivision does not apply to a publicly traded company); and
(3) the person or business entity, if any, that served as a compensated broker or intermediary to actively facilitate the applicable contract or negotiated the terms of the applicable contract with the state agency. (This subdivision does not apply to persons or business entities performing legal services related to the negotiation or drafting of the applicable contract.)

*"State agency"* means a board, commission, office, department or other agency in the executive, judicial or legislative branch of state government, including publicly funded institutions of higher education: Provided, that for purposes of W. Va. Code § 6D-1-2, the West Virginia Investment Management Board shall not be deemed a state agency nor subject to the requirements of that provision.

The contracting business entity must complete this form and submit it to the contracting state agency prior to contract award and to complete another form within 30 days of contract completion or termination.

*This form was created by the State of West Virginia Ethics Commission, 210 Brooks Street, Suite 300, Charleston, WV 25301-1804. Telephone: (304)558-0664; fax: (304)558-2169; e-mail: ethics@wv.gov; website: www.ethics.wv.gov.*

*Revised June 8, 2018*

West Virginia Ethics Commission

# Disclosure of Interested Parties to Contracts

(Required by *W. Va. Code* § 6D-1-2)

**Name of Contracting Business Entity:** ____________________ **Address:** ________________________________

________________________________

**Name of Authorized Agent:** ____________________________ **Address:** ________________________________

**Contract Number:** __________________________ **Contract Description:** ____________________________

**Governmental agency awarding contract:** ________________________________________________________

□ **Check here if this is a Supplemental Disclosure**

List the Names of Interested Parties to the contract which are known or reasonably anticipated by the contracting business entity for each category below *(attach additional pages if necessary)*:

1. **Subcontractors or other entities performing work or service under the Contract**
   □ Check here if none, otherwise list entity/individual names below.

2. **Any person or entity who owns 25% or more of contracting entity (not applicable to publicly traded entities)**
   □ Check here if none, otherwise list entity/individual names below.

3. **Any person or entity that facilitated, or negotiated the terms of, the applicable contract (excluding legal services related to the negotiation or drafting of the applicable contract)**
   □ Check here if none, otherwise list entity/individual names below.

Signature: ______________________________________ Date Signed: ______________________________

## *Notary Verification*

State of ____________________________________, County of ________________________________________:

I, ________________________________________________________, the authorized agent of the contracting business entity listed above, being duly sworn, acknowledge that the Disclosure herein is being made under oath and under the penalty of perjury.

Taken, sworn to and subscribed before me this ______________ day of _______________________, _____.

________________________________________________________
Notary Public's Signature

***To be completed by State Agency:***
Date Received by State Agency: ________________________________
Date submitted to Ethics Commission: ____________________________
Governmental agency submitting Disclosure: ________________________

*Revised June 8, 2018*