

Original



**Proposal For
CRFP 0212 SWC1900000001
Managed Voice Services**

**Prepared For
West Virginia
Department of Administration
Purchasing Division**

**Summer Bailey
Technology Solutions Executive
November 21, 2018**

RECEIVED

2018 NOV 26 PM 3: 17

WV PURCHASING
DIVISION

Getronics
CONNECTING POSSIBILITIES



**West Virginia
Department of Administration
Purchasing Division
CRFP 0212 SWC1900000001
Managed Voice Services**

Getronics

Summer Bailey
135 Corporate Centre Drive, Suite 410
Scott Depot, WV 25560
Phone: (304) 553-7526
Mobile: (304) 541-4288
Email: Summer.Bailey@getronics.com

Corporate Office

1020 Petersburg Road
Hebron, Kentucky 41048
www.getronics.com
Toll-Free: 800.846.8727
Federal Tax ID: 61-1352158

Addendum Acknowledgement

Getronics received:

Addendum 01 dated 10-19-2018
Addendum 02 dated 10-25-2018
Addendum 03 dated 11-2-2018
Addendum 04 dated 11-15-2018
Addendum 05 dated 11-16-2018

Delivery Information

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

Due: November 27, 2018 1:30PM EDT
Technical Copy and Separate Cost Copy
One Original and Five Copies
Label cartons or envelopes:

<p>Technical Proposal Sealed Bid: VOIP Managed Services Buyer: Mark Atkins Solicitation No. CRFP 0212 SWC1900000001 Date: November 27, 2018 Time: 1:30 PM Bidder: Getronics</p>	<p>Cost Proposal Sealed Bid: VOIP Managed Services Buyer: Mark Atkins Solicitation No. CRFP 0212 SWC1900000001 Date: November 27, 2018 Time: 1:30 PM Bidder: Getronics</p>
--	---



November 21, 2018

Getronics
1020 Petersburg Road
Hebron, KY 41048

Mark Atkins, Senior Buyer
2019 Washington Street, East
Charleston, WV 25305
Mark.A.Atkins@wv.gov 45701

Dear Mr. Atkins,

Getronics is pleased to submit this proposal to West Virginia Department of Administration, Purchasing Division (hereinafter referred to as the "Purchasing Division") for CRFP 0212 SWC1900000001 VOIP Hosted Services.

Note: On October 1, 2018, Pomeroy IT Solutions Sales Company, Inc. began doing business as 'Getronics', the name of our new parent company.

To provide the best solution for West Virginia government offices, Getronics chose to partner with **Cameo Global** for this response to the state. We guarantee all work and services provided by our partner in provision of this engagement. *'The Getronics team'* of Cameo and Getronics will meet and exceed West Virginia expectations.

This proposal is valid for 90 days. We are confident that we can meet your requirements for quality, timeliness and expertise. Please feel free to contact me if you have any questions or desire additional information.

Sincerely,

Summer Bailey
Technology Solutions Executive

Table of Contents

Headings	Page
Section 1 General Information.....	5
Section 2: Instructions to Vendors Submitting Bids	5
Section 3: General Terms and Conditions.....	6
Designated Contact.....	6
Certification and Signature	6
Definitions, Abbreviations, Acronyms	7
Section 4 Project Specifications	7
Attachments and Forms	37

Section 1 General Information

The Getronics team, understands and agrees to the General Information, as included in the RFP.

Section 2: Instructions to Vendors Submitting Bids

The Getronics team, understands and agrees to the Instructions to Vendors Submitting Bids, as included in the RFP.

Section 3: General Terms and Conditions

The Getronics team, understands and agrees to the General Terms and Conditions, as included in the RFP.

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.

Summer Bailey, Technology Solutions Executive

(Name, Title)	
Summer Bailey, Technology Solutions Executive	135 Corporate Centre Drive, Suite 410 Scott Depot, WV 25560
(Printed Name and Title)	(Address)
Phone: (304) 553-7526 / Mobile: (304) 541-4288 /	Email: Summer.Bailey@getronics.com
(Phone Number) (Fax Number)	(email address)

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.

Pomeroy IT Solutions Sales Company, Inc (d.b.a. Getronics)

(Company)

Robert Burlas VP Sales - East Central Region

(Authorized Signature) (Representative Name, Title)

Robert Burlas VP Sales - East Central Region November 20, 2018

(Printed Name and Title of Authorized Representative) (Date)

Phone: (317) 308-9060 / Email: Robert.Burlas@getronics.com

(Phone Number) (Fax Number)

Definitions, Abbreviations, Acronyms

Getronics and Cameo Global, (the Getronics team) have read and understand the information provided under this heading in the RFP.

Section 4 Project Specifications

The Getronics team read and understands the information under this heading. We offer the following responses to these 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, 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 (UCaaS 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 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.

The Getronics team has read and understands the information under this heading.

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.

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
2. Daily management, operational support, and ongoing maintenance of the State's current telephony environment, as outlined in Appendix_A.
3. MACD changes to the State's current telephony infrastructure.
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.

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

State Duties:

1. *Management of State's LANIWAN Network Infrastructure*
2. *Ordering, disconnecting, and billing services*

The Getronics team has read and understands the information under this heading.

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.

The Getronics team offers the following response. Our Getronics team has numerous individuals that has been helping customers implement new, and migrate and manage existing implementations, since 2001 – virtually the start of the modern voice over IP era. The team uses both modern methodologies and time-tested strategies that rely primarily on first listening to the customer, and then implementing standardized procedures that are customized to specific scalable and repeatable outcomes. With dozens of highly skilled engineers and highly skilled operations staff dedicated only to contact center and voice communications, our team understands and recognizes the challenges of legacy customer implementations.

4.2.1.1.1.3 *The State desires that the State and Vendor finalize 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.*

The Getronics team offers the following response:

The Getronics response team has already been sharing the contents and scope of this RFP with our operations team. We are prepared immediately to meet onsite with the State to discuss our initial plan. This team would consist of operational management, lead engineers, project managers, and administrative support staff. Loosely defined, our methodology is one of immediate task differentiation by triage, with the State actively defining our immediate priorities, timelines, and scope.

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.

The Getronics team offers the following response:

The Getronics team will respond with a team of experienced and dedicated Cisco voice and contact center specialists. This team has deep familiarity with the legacy components of the current State voice and contact center infrastructure. As such, the team will be multi-faceted. Some will begin immediate technical evaluations of the current implementation. Others will focus on the process and procedure of help-desk integration as it relates to size and scale. The team assigned to the State will not be generalists. Each person will have specific Cisco voice and contact center experience in Call Manager, UCCX, Cisco voice gateways, and MPLS / VPN technologies. As a team, we are organized in technical tiers, project management, operational experts, a dedicated customer relationship manager, and overall management.

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.

The Getronics team offers the following response. We will have local resources as part of the team dedicated to the State. Onsite resources are a critical part of the entire team of engineers, subject matter experts, project, and customer managers.

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.

The Getronics team offers the following response. The State's requests above are our primary method of help-desk interaction. Immediately upon execution, The Getronics team will meet with the State to develop a comprehensive triage process for support calls. That process will be integrated into our help-desk process, and escalation procedures established.

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.

The Getronics team offers the following response. The State's request is similar to many of our current customer base; managed legacy while transitioning to our hosted offerings. Getronics has found that constant communication with our customer's stakeholders is key. All impacted parties must have accurate information available to them – site end users, site management, IT, executive management, and customer administrative staff. The Getronics project and customer relationship managers will

customize our existing processes to enable the State to process migrations with a minimum of disruption to the public and the State.

4.2.1.1.2.2 The Vendor should include site preparation and coordination services to implement a turn-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.

The Getronics team offers the following response. We have read and understand the requirements listed above. At a high level, the listed items are standard operating procedure for our team. As noted previously, the key to successful migrations are early communication with the State with regards to the specifics of their requirements. As such, The Getronics team will customize our standard procedures early to ensure migrations, documentation, process and procedure are understood and consistently executed.

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 (VOJP) 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.

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.

The Getronics team offers the following response:

Based on the State's stated desire to provide a UCaaS solution to their user base, the Getronics team will expand our existing and reliable UCaaS platform based on proven and scalable Cisco technology, customized to be cost-effectively delivered with the State's packages as described. For the purposes of this proposal, the package terminology will be rereferred to as Basic (Basic), Foundation (Enhanced), and Standard (Premium). The requested features will be provided as listed in this RFP.

4.2.1.1.3.2 The State desires six handset options for use under this contract: a 2-line phone, a 6-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.

The Getronics team offers the following response:

A full range of handsets will be available for lease as requested. Final models will be determined based on the specific user needs and vendor availability at the time of migration to our UCaaS solution or at a request for replacement. All model types and requirements stated in this RFP are available and terms agreed.

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.

The Getronics team offers the following response:

The proven Cisco based UCaaS solutions offered by Getronics are fully compatible with existing Cisco SRST hardware for sites. At the time of migration to a UCaaS solution, at the State's option, Getronics will either use the existing SRST equipment and modify the configuration to the UCaaS solution or replace and configure the equipment per a State refresh program. For SRST and local 911 calling to remain functional, a local POTS or equivalent service will be required, which can be standard Analog or a fractional PRI.

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.

The Getronics team offers the following response:

The proposed solution is in compliance with this request. "On-net" calling does not technically require additional per call charges and our solution does anticipate on-net call charges. As required for any Voice over IP (VoIP) solution, sufficient network bandwidth and voice quality settings applied must be in place to handle the total call volume requested per site.

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 mls latency or better, and jitter of 40 mls or better. Please describe your network engineering architecture and your practices to continuously achieve these standards.

The Getronics team offers the following response:

The proposed solution provides connections to virtually any standard PSTN provider (a telco) and subsequent network-based connections in the formats this proposal requires. This includes Cloud based call termination into the UCaaS solution via SIP termination, a centralized SIP trunk solution within the State's datacenters, or local PSTN connections at a site. The solution is also able to handle a nearly infinite combination of these solutions as well. Final trunk and network sizing are based on the total concurrent estimated call volume for a particular location or network.

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 Attachment A Cost Sheet for both one-time installation costs and for monthly recurring costs for these connections. Please describe your ability to meet this goal.

The Getronics team offers the following response:

The proposed solution is in compliance with this request. The Getronics UCaaS solution offers direct MPLS connections into our geographical diverse datacenters (Columbus, Ohio and Ft. Worth Texas) for efficient routing of traffic from sites to the UCaaS solution. MPLS can be delivered on Getronics sold circuits or leverage existing State contracts to place existing or upgraded telco MPLS solutions in our datacenters.

These types of solutions have been deployed within Getronics UCaaS solution for years, and the Getronics team is well-versed in MPLS interoperability with best practice routing.

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.

The Getronics team offers the following response:

The proposed solution is in compliance with this request. Our UCaaS solution offers several methods to complete the above request. For our initial and primary response,

the solution proposes Cisco Expressway to provide SSL/TLS encrypted phone registration and call capabilities.

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.

The Getronics team offers the following response. Our proposed solution is in compliance with this request.

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.

The Getronics team offers the following response. Our proposed solution is in compliance with this request.

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 its per minute international calling rates for Mexico, Canada, and Jamaica in the Attachment_A Cost Sheet. These will be used as part of the cost evaluation. The Vendor should also attach an appendix of its international calling rates for all countries. This appendix will be used to establish the international calling rates per country in the awarded contract and will be required prior to award. Please describe your solution's international calling offerings.

The Getronics team offers the following response. Our proposed solution is in compliance with this request.

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.

The Getronics team offers the following response. Our proposed solution is in compliance with this request.

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.

The Getronics team offers the following response. Our proposed solution is in compliance with this request. As an integral part of our UCaaS solution, inbound traffic is dispersed in a fully active/active, load balancing solution between geo-redundant sites. Sizing is based to 100% of the total concurrent call volume per site to allow processing of calls in the highly unlikely event of a failure or issue within one of the datacenters, or the overall network

Within the State's network, our solution will automatically take advantage of redundant routing and various voice and quality of service prioritization settings.

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 CPS/ALI)services for 911 calls. Please describe your process for ensuring the accuracy of 911 call delivery, as well as the process to support PSALI.

The Getronics team offers the following response. Our proposed solution is in compliance with this request. The UCaaS solution as part of the base solution uses location based 911 calling to route emergency calls with priority over location local PSTN connections. In the event that a local PSTN connection is not available, the 911 will be routed over centralized trunks with the local PSTN number as the outbound ANI to provide location recognition for emergency services. Additional options are available for enhanced 911 routing as an optional service.

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.

The Getronics team offers the following response. Our proposed solution is in compliance with this request.

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.

The proposed solution is in compliance with this request. The UCaaS solution provides scalability for concurrent calls on at the request of the State agency. The scalability can be provision generally the same day as the request.

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.

The Getronics team offers the following response. Our proposed solution is in compliance with this request.

4.2.1.1.3.17 The Vendor's solution should provide the following quality and reliability standards: QoS tagging IEEE 802.1Q-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.

The Getronics team offers the following response. Our proposed solution is in compliance with this request.

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.

The Getronics team offers the following response. Our proposed solution is in compliance with this request. As part of the base UCaaS deployment, integration with O365, Microsoft Exchange, and other 3rd party email solutions are provided, based on the license level of the end user. Retention policies for voicemail are set as part of the class of service for the end user and can be set to a requested period of time. Email retention of voicemails are controlled by the email solution and email vendor. In addition, the Cisco UCaaS solution is capable of being integrated to Active Directory via LDAP integration. Contact Center solutions are capable of using Active Directory Federated 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.

The Getronics team offers the following response. Our proposed solution is in compliance with this request. The UCaaS solution provides paging services through vendor-maintained components. Integration to over-head paging systems is provided through existing or net new Analog device adapters and will be engineered on a per location discovery and onboarding process.

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.

The Getronics team offers the following response. Our proposed solution is in compliance with this request. The UCaaS solution provides optional licensing for Operator Console services. Licensing is provided on a concurrent operator basis.

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.

The Getronics team offers the following response. Our proposed solution is in compliance with this request. In general terms, the Cisco UCaaS solution can be integrated with any Cisco Supported third-party call recording solution. Additional discovery and engineering is required to provide final solution requirements to complete this specific request.

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.

The Getronics team offers the following response. Our proposed solution is in compliance with this request. The UCaaS solution is capable of supporting Cisco generation 2 and later IP telephony handsets. Generation 1 models are no longer supported on Cisco solutions, which include model 12, model 30, 7902, 7905, 7910, 7912, 7920, 7921, 7935, 7970, 7971. Specific Cisco supported device documentation can be supplied at request.

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 PH). For ease of deployment and maintenance, the State prefers the contact center solution be web-based. The solution should provide the following capabilities:*

Required Capabilities	Provided
<i>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</i>	Yes
<i>Should provide chat capabilities</i>	Yes
<i>Should provide live data reporting</i>	Yes
<i>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</i>	Yes
<i>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</i>	Yes
<i>Should provide scalability for up to 800 agents and the ability to expand in the future</i>	Yes

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

The Getronics team offers the following response. Our proposed solution is in compliance with this request.

The HCS (Hosted Contact Center Solution) provides Chat and Email capabilities as part of the agent license from Cisco. This solution allows a single interface for blended or dedicated agents to handle all configured interactions with customers while the underlying system is aware of the interaction type the agents are handling. Intelligent business rules can be developed to allow agents to handle interactions by priority, type, or manually.

Live data gadgets are provided based on roles and configuration to agents and supervisors for teams to understand or manage the specific interactions they are able to handle.

The Cisco IVR solution is callable of interfacing with virtually any database type to provide routing decisions, and/or populate information to an agent workspace. Optionally screen-pop capabilities are available to standards-based web application, or to custom desktop based applications through additional engineering, discover, and development.

Cisco provides additional agent options for PSTN connectivity to telephones via a solution called Mobile Agent. With Mobile Agent, users login to an VPN service that provides access to the agent desktop environment and enters a properly formatted PSTN number. Calls are then routed to the PSTN number for customer handling.

The Cisco HCS environment is capable of expanding to 2,000 agents as part of the base deployment and is capable of being expended to 12,000 agents if required.

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.

The Getronics team offers the following response. Our proposed Cisco HCS solution is based on the Cisco Unified Contact Center Enterprise (UCCE) solution. This proposal provides a fully active/active infrastructure that is located in Columbus, OH and Dallas, TX. The architecture is designed in a way that any hosted component can fail, and the other active side can assume control without manual interference. Sizing of components are built to provide the ability to handle 100% of the call volume on either side of the solution, and calls are processed on both sides at the same time so that in the unlikely event of a failure, processing is assumed by the other side. This allows critical service delivery through most disaster scenarios. In the event of a failure on a device that is actively controlling the call, such as a voice gateway, or an agent phone, there is no ability to move that call to another device, and active calls may be dropped, but the next call will be answered by redundant equipment. These unlikely events can be mitigated by final solution architecture and design.

Upgrades to the HCS environment are handled by Cisco best practices and can be completed with either zero or momentary down time due to the active/active nature of the solution.

The vendor datacenters where the HCS environments are located are placed in the highest service tier with fully redundant power, communication infrastructure and located in datacenters with high security standard.

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:

Enhanced Features	Provided
<i>Agent and Supervisor client that provides Blended agents: Inbound and outbound capability</i>	Yes
<i>Ability to monitor critical performance metrics</i>	Yes
<i>allowing managers to coach, train, and encourage agent behavior</i>	Yes
<i>Ability for Supervisors to change an agent's status</i>	Yes
<i>Ability for Supervisors to silently monitor inbound and outbound calls</i>	Yes

Enhanced Features	Provided
Ability to interrupt an agent's call to interact with both the caller and the agent	Yes
Ability for Supervisors to remove an agent from a call	Yes
Ability to change an agent's skill profile in real time	Yes

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

The Getronics team offers the following response. Our proposed solution is in compliance with this request. The proposed HCS solution provides all the above capabilities as part of the based platform either through the agent and supervisor workspace, or through the reporting platform that is provided with the Contact Center solution.

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, PH, 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.

The Getronics team offers the following response. Our Getronics team has deep capabilities in configuring, and if necessary, customizing call recording solutions compatible with Cisco solutions. We have experience with multiple vendors, their APIs, desktop, network, and/or built-in-bridge capabilities. Moreover, the proposed solution has been well vetted in terms of network bandwidth, reliability, and fault-tolerance.

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.

The Getronics team offers the following response. Our proposed solution is in compliance with this request. The HCS solution provides two primary ways to provide outbound campaigns. The Cisco solution has an out of the box dialer capability but does not provide in-depth campaign management tools. Additional vendor provided tools are available to provide full outbound campaign management capabilities including web-based supervisor scheduling and maintenance of campaigns, integrated agent scripting per campaign, do not call lists, zip code time shifting, automation of phone dialer lists, and many more.

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.

The Getronics team offers the following response. Our proposed solution is in compliance with this request. The proposed solution is certified compliant to PCI v3.2

and HIPPA by PCI approved QSA ControlCase. Further, ControlCase certified Getronics System and Organizational Controls under the SSAE 16 standard; SOC1 Type1, SOC1 Type2, SOC2 Type1, and SOC2 Type2. The link to the ControlCase website with the solutions listed as compliant with PCI-DSS v3.2 is:
<https://seal.controlcase.com/index.php?page=showCert&cld=4678918700>

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.

The Getronics team offers the following response. Within a strict IT governance framework, Vendor maintains a full library of documented policies and procedures, on a schedule for periodic review, with Information Security, Change Management, Incident Management, Problem Management, and Risk planning at its core. For the goal of providing a secure solution that delivers confidentiality, integrity and availability, the proposed solution meets or exceeds industry standards.

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.

The Getronics team offers the following response. Executive leadership mandates and supports thorough governance that includes cyber security in order to preserve confidentiality, integrity and availability of all systems and data, with emphasis on sensitive data. This is successfully achieved through a continuous review and improvement of security and privacy controls (NIST 800-53, ISO 27001), including 1) holistic and structured enterprise risk planning that transcends strictly IT infrastructure and personnel, 2) periodic security verification through internal audits and outsourced control & penetration testing, and 3) documented breach planning, including distribution lists & templates for notifications, and periodic training.

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.

The Getronics team offers the following response. Following the end of each calendar month of the Subscription Term under an Order Form, Getronics measures the "System Availability Level" over the immediately preceding month.

Getronics can provide this report out of band with three business days' notice. These reports should be requested as a Service Request via the Getronics customer support portal.

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.

The Getronics team offers the following response. In the course of the on-boarding process to Getronics services, our team engages with the customer to develop a standard cadence of meetings. A typical Getronics service lifecycle consists of:

- During the Architecture/Design/Implementation phase of a new service or solution- no less than weekly Project Management meetings.
- Post implementation - no less than semi-monthly service review meetings. These meetings will address Ordering / Billing and Service / Support

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.

The Getronics team offers the following response.

During the on-boarding process to Getronics services, our team engages with the customer to develop a notification list and process for service impacting incidents. This list is incorporated into our standard operating procedure (SOP) for each customer and is reviewed quarterly with the customer to ensure that contact information is current. Updates to the contact list are re-incorporated into Getronics's SOP for the customer.

Upon validation of a service impacting incident, the Getronics team attempts to reach key customer contacts by phone to alert them of the event. A standard written notification is then sent to the customer contacts; this notification details the impact to the customer environment, steps being taken to restore service and either an estimated time of service restoration or the time the customer should expect the next the expected time of the next update communication from the Getronics team.

When a service impacting (Severity 1) incident has been closed, Getronics will provide a detailed Root Cause Analysis report to the impacted customers. This RCA document contains an Impact Summary, Incident Resolution/Root Cause and Recommendations/Remediation steps.

4.2.1.3.4 Vendor should provide written notification often (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.

The Getronics team offers the following response. During the on-boarding process to Getronics services, our team engages with the customer to develop a notification list and process for service impacting incidents. This list is incorporated into our standard operating procedure (SOP) for each customer and is reviewed quarterly with the customer to ensure that contact information is current. Updates to the contact list are re-incorporated into Getronics's SOP for the customer.

Getronics categorizes maintenance into 3 classifications: Planned, Priority and Emergency.

Approximately 2 calendar weeks prior to planned maintenance, Getronics distributes a standard written notification to the customer contact. This notification details the date and time of the maintenance window, items that the maintenance will be addressing and the expected impact to the customer environment. At the beginning of the scheduled maintenance window, the Getronics team sends a standard "Maintenance is beginning" notification to the customer team; at the conclusion of maintenance activities, the Getronics team sends a standard "Maintenance has ended" notification.

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 company's notification process for emergency maintenance and outages.

The Getronics team offers the following response. Getronics categorizes maintenance into 3 classifications: Planned, Priority and Emergency.

Priority maintenance is defined as a sub-optimal situation that presents some risk to the customer environment but has not resulted in a degraded or impaired state. Getronics invokes a Priority maintenance window when in our professional and experiential judgement the situation cannot wait for normally scheduled maintenance. Getronics makes every effort to minimize the occurrence of Priority Maintenance activities and the impact to customer environments. When possible, Getronics strives to provide at least 2 days' notice to customers prior to Priority maintenance activities.

Emergency maintenance is defined as an Incident, issue or condition that has caused a severe impact and requires immediate attention. Issues that are serious but have a short-term work around are also considered emergency, however maintenance is typically performed the same day, but in a lesser impacting time frame.

Getronics distributes a standard written notification to customer teams at the beginning and end of all maintenance activities, regardless of the maintenance classification.

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.

The Getronics team offers the following response. As part of Getronics's ongoing regular communications with customers, on-site visits will be planned according to the customer's requirements.

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.

The Getronics team offers the following response. Getronics has instituted a three-tier support structure in which all technicians are proficient in spoken and written English. All Incidents are triaged by Tier 1 technicians and escalated to Tier 2 / Tier 3 technicians based on severity of the issue, impact to the customer environment and length of time open. Upon confirmation of a Sev1/Sev2 incident, Tier 2 / Tier 3 technicians are immediately engaged to begin service restoration. Service notifications are also generated and distributed to the Getronics operations/support and management teams as well as to key customer contacts.

When a ticket is assigned to a technician, the technician holds responsibility for the entire life cycle of the ticket including coordinating communications, activities and escalations until the issue has been resolved.

Getronics also completes daily service reviews of open Incidents for all accounts to ensure that each Incident and customer are receiving proper attention.

Getronics regularly completes internal Root Cause Analysis process for Critical incidents, a Root Cause Analysis detailing the Incident Impact/Summary, Resolution and Remediation/Recommendations is generated and supplied to the impacted customer(s).

As part of Getronics's Continuous Improvement program, ticket review and analysis is completed for select non-critical incidents.

Each Getronics CloudBlu (hosted solution) and Managed Service customer is provided a monthly report detailing Incident and Service Request information.

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.

The Getronics team offers the following response detailing our severity level structure:

Severity 1

The Customer's Service is critically impacted. More than 75% of individuals, sites or devices are not functional and operations are very limited. Examples of a Severity 1 incident include but are not limited to:

- A specific Service is not functioning for the entire company
- No calls can be received at any site of the company
- No calls can be initiated at a site of the company
- Contact Center is not functional for critical business units

Getronics will provide support 24x7 until the Severity 1 incident is resolved, or a solution (work-around) to restore service is implemented. Customer must provide Getronics with a contact during this 24x7 period to assist with data gathering, testing, and applying fixes.

Severity 2

The Customer's Service is severely impacted. More than 50% of individuals, sites or devices are impacted and are not fully functional, however operations can continue in a restricted fashion. Examples of Severity 2 incidents include but not limited to:

- A specific Service is partially functioning for the entire company
- No calls can be received at a branch site of the company
- No calls can be initiated at a branch site of the company
- Contact Center is not functional for a group of agents or a queue

Getronics will provide support 24x7 until the Severity 2 incident is resolved, a reasonable work-around is put in place, or as long as useful progress can be made. Customer must provide Getronics with a contact during this 24x7 period to assist with data gathering, testing, and applying fixes.

Severity 3

The Customer's Service experiences a minor loss of service or disruption to operations. The impact is an inconvenience, however normal operations can continue. Examples of Severity 3 incidents include but not limited to:

- A user cannot receive calls
- A user cannot initiate calls
- Password needs to be reset
- An agent cannot log into the Contact Center application

Getronics will provide support during normal business hours to resolve the Severity 3 incident or restore functionality through a work-around or as long as useful progress can be made. Customer must provide Getronics with a contact during Getronics normal business hours to assist with data gathering, testing, and applying fixes.

Severity 4

The Customer's Service is operating as expected and Customer experiences no loss of service as defined in the initial, mutually agreed UAT period. The Customer requests information, enhancement, or documentation clarification regarding the Service. Getronics will work during normal business hours to address the Severity 4 service request.

Getronics's policy to Service Request severity level changes is as follows:

Initial Severity Level

At the time Getronics accepts an incident report, Getronics will record an initial severity level of the incident based on the above severity definitions. Getronics's initial focus, upon acceptance of an incident report will be to restore service by resolving the underlying issue or applying a work-around. The severity level of an incident may be adjusted as described below.

Downgrade of Incident Levels:

If, during the incident management process, the issue no longer warrants the severity level currently assigned based on its current impact on the production operation of the applicable Service, then the severity level will be downgraded to the severity level that most appropriately reflects its current impact and the Customer will be immediately notified.

Upgrade of Incident Levels:

If, during the incident management process, the issue warrants the assignment of a higher severity level than that currently assigned based on the current impact on the production operation of the applicable Service, then the severity level will be upgraded to the severity level that most appropriately reflects its current impact.

Adherence to Severity Levels definitions:

Customer shall ensure that the assignment and adjustment of any severity level designation is accurate based on the current impact on the production operation of the applicable Service. Customer acknowledges that Getronics is not responsible for any failure to meet performance standards caused by Customer misuse or mis-assignment of severity level designations.

Incident Escalation

For incidents where the Customer desires an increase in escalation level(s), the Getronics support analyst will engage the Getronics incident escalation representative who will be responsible for managing the escalation. The Getronics incident escalation representative will work with Customer to develop an action plan and allocate the appropriate Getronics resources. If the issue underlying the incident continues to remain unresolved, Customer may contact the Getronics incident escalation representative to review the incident and request that it be escalated further. To facilitate the resolution of an escalated incident, Customer and Getronics shall provide contacts within Customer's organization that are a level reasonably appropriate to address the severity of the escalated incident.

Getronics's Service Level Objective Policy is as follows:

Mean Time to Respond (MTTR)

Defined as the time taken to respond to a Customer's request. Measured from the time the request is made from the Customer to the time Getronics responds to the request.

- Severity 1: 30 Minutes
- Severity 2: 2 Hours
- Severity 3: 1 Business day
- Severity 4: 2 Business days

Mean Time to Notify (MTTN)

Defined as the average time taken to notify Customer of an issue. Measured from the time that an alarm is generated to notify the Getronics network operations center of an issue, to the time that it takes to notify Customer Contact. Getronics's MTTR target is less than 20 minutes per incident.

Mean Time to Restore Service (MTRS)

Defined as the average time taken to restore service after a failure. Measured from when the service fails until it is fully restored and delivering its normal functionality. MTRS targets to restore service to the previous known working configuration are based on the priority level of the incident as follows:

- Severity 1: 4 hours
- Severity 2: 12 hours

- Severity 3: 2 business days
- Severity 4: 5 business days

Moves, Adds, Changes and Deletions (MACD)

End User MACD services may be performed by the Customer or optionally by Getronics. End User MACD services are optional and will be noted as a separate monthly item on the Sales Form.

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*

The Getronics team offers the following response. Our Getronics has developed and utilized standard order forms for use by customers to request changes to services. Service changes and requests are included in Getronics's monthly reporting to customers.

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.

The Getronics team offers the following response. Our proposed solution is in compliance with this request. The proposed solution provides a web portal for generating vendor requested MACD changes as well as a self-service portal to make simple MACD changes based on training provided to authorized State staff if desired. This solution provides reporting on overall service levels, tickets opened, tickets completed, and solution requirements that can be delivered on a pre-determined schedule to authorized management staff.

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.

The Getronics team offers the following response. Our proposed solution is in compliance with this request. The proposed solution includes training for each type of user which can be delivered in a recorded format for integration into the State LMS. Train the trainer session are part of the proposed solution and additional training can be requested as part of the ongoing project request process.

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.

Our proposed solution is in compliance with this request.

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 requirements are exceeded, will be included in technical scores where appropriate. The mandatory project requirements are listed below.*

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.*

The Getronics solution provides 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 of the RFP, through the migration period to a Hosted VoIP solution. Additionally, at the State's discretion, Getronics will migrate any site to the hosted solution through the formal Change Request in the formal Statement of Work that governs the engagement.

4.2.2.2 Hosted Voice Services

Requirement	Supported
4.2.2.2.1 <i>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.</i>	Yes
4.2.2.2.2 <i>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.</i>	Yes

Requirement	Supported
4.2.2.2.3 Vendor's solution must provide local telephone numbers in West Virginia.	Yes
4.2.2.2.4 Vendor's solution must support inbound Automatic Number Identification (ANI).	Yes
4.2.2.2.5 Vendor's solution must include inbound Caller ID, outbound custom telephone number, and outbound custom name display.	Yes
4.2.2.2.6 Vendor's solution must support Dialed Number Information Services (DNIS) on 800 # toll-free telephone services.	Yes
4.2.2.2.7 Vendor's solution must support rerouting of calls to an alternate site at the State's directive.	Yes
4.2.2.2.8 Vendor's solution must support 900/976 blocking.	Yes
4.2.2.2.9 Vendor's solution must support x11 services (currently 211,411,511,611, 811,911).	Yes
4.2.2.2.10 Vendor's solution must include Direct Inward Dial (DID) feature and service,	Yes
4.2.2.2.11 Vendor's solution must support Operator services.	Yes
4.2.2.2.12 Vendor's solution must support local number portability.	Yes
4.2.2.2.13 Vendor's solution must provide unlimited free local and long-distance calling.	Yes
4.2.2.2.14 Vendor's hosting center(s) must be located within the continental United States.	Yes
4.2.2.2.15 Vendor must provide Train the Trainer sessions for Hosted Voice Services implementations.	Yes

The proposed solution is in compliance with this above request table. All requested functionality is provided in the proposed solution.

4.2.2.3 Hosted Contact Center Services

Vendor's Contact Center solution must support:

Requirement	Supported
4.2.2.3.1 Automatic Call Distributor (ACD)	Yes
4.2.2.3.2 Computer telephony integration (CTI)	Yes
4.2.2.3.3 Call control	Yes
4.2.2.3.4 E.164	Yes
4.2.2.3.5 Interactive voice response (IVR)	Yes
4.2.2.3.6 Voice Recording	Yes
4.2.2.3.7 High Availability with load balancing and built-in redundancy	Yes
4.2.2.3.8 Vendor must provide Train the Trainer sessions, encompassing all Hosted Contact Center roles - Administrator, Supervisor, and Agents.	Yes

The proposed solution is in compliance with this above request table. All requested functionality is available in the proposed solution. Specific requirement such as CTI capabilities require additional discovery and documentation to provide a final solution.

4.2.2.4 Security

Security Requirement	Agree
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.	Yes
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: https://technology.wv.gov/security/Pages/policies-issued-by-the-cto.aspx	Yes
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:	Yes
<ul style="list-style-type: none"> Health Insurance Portability and Accountability Act (HIPAA) requirements as outlined in the attached Business Associate Addendum (BAA) (see Attachment B) 	Yes
<ul style="list-style-type: none"> 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; 	Yes
<ul style="list-style-type: none"> Family Education Rights and Privacy Act (FERPA) requirements; 	Yes
<ul style="list-style-type: none"> Criminal Justice Information System (CnS) requirements; 	Yes
<ul style="list-style-type: none"> Payment Card Industry Data Security Standards (PCI-DSS) requirements; 	Yes
<ul style="list-style-type: none"> Federal tax Information (FTI) and Internal Revenue Service publication 1075 (IRS 1075) requirements; 	Yes
<ul style="list-style-type: none"> Centers for Medicare & Medicaid (CMS) Services Information Security Policy requirements. 	Yes
<ul style="list-style-type: none"> Ensure network boundary and access control protection such as dual session boundary controllers and firewalls. 	Yes
<ul style="list-style-type: none"> Data-at-rest and data-in-transit encryption. 	Yes
<ul style="list-style-type: none"> Role-based access control for all applications which process and/or store sensitive data, to ensure need-to-know policies are enforceable. 	Yes

The proposed solution has demonstrable certifications for PCI, HIPAA, and SOC Type 1 and Type 2 standards. FISMA and FERPA overlap these standards. CMS relies largely on FIPS 199, and our solution conforms to those standards. To the extent CnS relies heavily on the aforementioned standards, we are compliant with CnS.

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.

The Getronics team read and agrees to the above requirement. We will provide the cyber risk management plan prior to the first implementation of our hosted solution.

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.

The Getronics team read and agrees to the above requirement. We will provide the incident management plan prior to the first implementation of our hosted solution.

The Vendor Incident Management Plan conforms to NIST SP 800-61rev2 requirements, although response forms are tailored to HIPAA and may need to be amended.

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.

The Getronics team read and agrees to the above requirement.

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.

The Getronics team read and agrees to the above requirement whereby NIST standards complement PCI, HIPAA, SOC standards. We will provide documentation of our compliance with those security standards.

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.

The Getronics team read and agrees to the above requirement for Service and Support.

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?chap=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.

The Getronics team read and agrees to the above requirement for Service and Support.

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.

The Getronics team read and agrees to the above requirement for Service and Support.

4.2.2.5.4 Vendor must work with the WVOT using the established Telecommunications Change Request (TCR) (Attachment_ C) procedures for ordering and implementing these telecommunications services.

The Getronics team read and agrees to the above requirement for Service and Support.

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.

The Getronics team read and agrees to the above requirement for Service and Support.

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.

The Getronics team read and agrees to the above requirement for Service and Support.

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.

The Getronics team read and agrees to the above requirement for Service and Support.

4.2.2.5.8 The Vendor must provide and update a weekly status report and/or order log for submitted TCRs.

The Getronics team read and agrees to the above requirement for Service and Support.

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.

The Getronics team read and agrees to the above requirement for Service and Support.

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.

The Getronics team acknowledges our acceptance of the above requirement for Service and Support.

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.*

The Getronics team offers the following response. We have 15+ years of experience designing, implementing and supporting Cisco voice and contact center solutions for a broad mix of customer verticals. Cisco maintains a very strict and audited certification process to ensure the partner of record is not only qualified but exceeds the minimum requirements to support the overall solution.

Company Certifications:

- Cloud & Managed Services Master
- Unified-Communication-as-a-Service (HCS)
- Contact-Center-as-a-Service (HCS)
- Advanced Collaboration Partner
- Advanced Technology Partner (ATP) Contact Center Enterprise

Cisco Partner Locator- Certification Website

<https://locatr.cloudapps.cisco.com/WWChannels/LOCATR/openBasicSearch.do?dtid=osscdc000283>

Staff Certifications

Getronics Engineering teams carry all relevant individual certifications required to carry the Cisco Certifications. These include CCIE, CCNA, CCNP, Voice & Contact Center Engineering Certifications. PMO teams maintain industry leading PMP & ITIL certifications.

Project Example: -Large Healthcare Equipment Provider, located in Lake Forest, CA. Project deliverable was to convert 5,000 global contact center agents to our cloud solution. Implementation was a phased rollout over 18-24 months, a dedicated team of 6-10 engineers, PMO and deployment resources completed the successful rollout in 2016-2017 timeframe. Goal was to streamline customer care expenses, deliver higher value channels of communication, improve system reliability while providing a higher level of redundancy.

4.3.1. Qualification and Experience Information: 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.

The Getronics team offers the following response. Our **Large Fortune 500 Technology Corp** - A customer managed services offering that has been in place for over 18 years for deploying and managing global IT infrastructure (datacenter, voice, firewalls, servers, etc.) Customer has over 300 global offices. Project goals include lifecycle infrastructure refreshments, upgrades, migration to other offices, optimization and break/fix services. Contract is still in force and in 2017 we expanded our services offerings to include 24/7 monitoring.

Global Medical Instrument Company- 3-year-old customer contract that provides full services managed services, help desk support and implementations to global company with over 200 locations. 2017 included 15 office refreshes in Europe supporting over 3,000 endpoints. Migration services in the US locations are planned for 2019-2020 timeframe.

Large Healthcare Equipment Provider- Our team provides managed services for over 5,000 voice endpoints with locations in the US and India. Deployment timeframe was 18 months and included providing management and monitoring services. Customer is in the process of working to migrate the voice to our cloud offering, project timeline is 2019-2020.

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.

The Getronics team offers the following response. Our **Large Healthcare Equipment Provider**- Cloud customer since 2016 has over 5,000 global contact center agents. Implementation was a phased rollout over 18-24 months, a dedicated team of 6-10 engineers, PMO and deployment resources completed the successful rollout in 2016-2017 timeframe. Goal was to streamline customer care expenses, deliver higher value channels of communication, improve system reliability while providing a higher level of redundancy. Services are still in place and actively looking to expand with us on adding more voice endpoints, all contact center agents 100% on our cloud service today.

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 staffs experience in working in these roles.

The Getronics team offers the following response. Our All aspects of our team will be engaged at some point with our large cloud and managed services clients. We proud ourselves on leveraging the sum of the parts and the unique skills of each of our individual contributors to deliver exceptional customer services and support.

Account Team- Single point of contact for customer relationship both in terms of sales and technical engineering services. Responsibilities include: Identifying new revenue opportunities, consulting with customer on optimization services, managing technical, business and executive relationships. Overall tasked with ensuring customer satisfaction

Implementation Team- Includes VP of Deployments, Implementation Engineers, Project Manager. They own the successful fulfillment of the business and technical deliverables and ensuring a timely and on-budget overall project. Roles include discovery, implementation, User Acceptance Testing, Training, Go-Live, Day 2 support and seamless handover to operations.

Operations- Teams include billing, technical support, Customer Success Manager, Ops Vice-President. Responsible for troubleshooting, bug fixes, upgrades, 24/7 monitoring, reporting services and optimization services.

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.

At the end of this proposal, the Getronics team included our Risk Assessment Policy.

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.

At the end of this proposal, the Getronics team included our Information Security Policy.

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 HIP AA, CMS, FERP A, cns Security Policy, PCI Data Security Standards (DSS), IRS Publication 1075, FISMA, NIST 800-53, NIST SP 800-171, and FIPS 200 if they apply.

The Getronics team offers the following response. Our PCI DSS 3.2

4.3.1.7 Vendor should provide a detailed list of the third-party attestations, reports, security credentials (e.g., FedRamp), and certifications relating to cybersecurity and privacy controls.

The Getronics team offers the following response.

- Current with PCI DSS 3.2
- Current with HIPPA
- Current with SOC1 & SOC2 Type2

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.

The Getronics team offers the following response. Our Getronics has extensive experience and processes for preparing, completing and maintaining both vendor audits and security compliance projects. Getronics has dedicated resources whose sole job responsibilities are to maintain these certifications and to ensure our company passes audits, maintains all documentation and provides our clients with the necessary policies and procedures to support their internal security policies and to ensure Getronics as a Solution Provider adheres to industry security compliance.

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.

At the end of this proposal, the Getronics team included our Information Security Policy.

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.

The Getronics team read, understands and agrees to provide the above requested information and demonstration during Oral Presentations.

Attachments and Forms

Getronics has included the following completed forms and attachments for our proposal.

- Purchasing Affidavit
- Ethics Disclosure Interested Parties
- Final_CRFP_0212_SWC1900000001_1_CRFP_FORM.PDF
- Final_CRFP_0212_SWC1900000001_2_CRFP_FORM ADD 1.PDF
- Final_CRFP_0212_SWC1900000001_2_CRFP_FORM ADD 2.PDF
- Final_CRFP_0212_SWC1900000001_4_CRFP_FORM ADD 3.PDF
- CRFP SWC1900000001 Addendum_4.pdf
- Cameo Global - Information Security Policy v18.4.pdf
- Cameo Global - Risk Assessment Policy_v18.2.docx.pdf
- Getronics Insurance COI Nov 2018.PDF

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFP 0212 SWC190000001

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)

- | | |
|--|--|
| <input checked="" type="checkbox"/> Addendum No. 1 | <input type="checkbox"/> Addendum No. 6 |
| <input checked="" type="checkbox"/> Addendum No. 2 | <input type="checkbox"/> Addendum No. 7 |
| <input checked="" type="checkbox"/> Addendum No. 3 | <input type="checkbox"/> Addendum No. 8 |
| <input checked="" type="checkbox"/> Addendum No. 4 | <input type="checkbox"/> Addendum No. 9 |
| <input checked="" type="checkbox"/> Addendum No. 5 | <input type="checkbox"/> 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.

Pomeroy IT Solutions Sales Co Inc
dba Getronics Company

Robert Butlaw

Authorized Signature

11/26/2018

Date

NOTE: This addendum acknowledgment should be submitted with the bid to expedite document processing.



Purchasing Division
 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 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:
 Pomeroy IT Solutions Sales Company, Inc. (dba Getronics)
 1020 Petersburg Road
 Hebron, KY 41048
 Robert Burlas, VP Sales South Central Region
 Phone: (317) 308-9060 / Email: Robert.Burlas@getronics.com

FOR INFORMATION CONTACT THE BUYER

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

Signature X *Robert Burlas* FEIN # 61-1352158 DATE Nov 15, 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 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
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 VARIOUS LOCATIONS AS INDICATED BY ORDER		STATE OF WEST VIRGINIA 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			

Item 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

SWC1900000001	Document Phase Final	Document Description RFP for Managed and Hosted Voice Services (OT18027)	Page 3 of 3
----------------------	---------------------------------------	---	------------------------------

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions



Purchasing Division
 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 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:
 Pomeroy IT Solutions Sales Company, Inc. (dba Getronics)
 1020 Petersburg Road
 Hebron, KY 41048
 Robert Burlas, VP Sales South Central Region
 Phone: (317) 308-9060 / Email: Robert.Burlas@getronics.com

FOR INFORMATION CONTACT THE BUYER

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

Signature X *Robert Burlas* FEIN # 61-1352158 DATE Nov 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.
3. 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 VARIOUS LOCATIONS AS INDICATED BY ORDER		STATE OF WEST VIRGINIA 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		

Item Code	Manufacturer	Specification	Model #
.61700			

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

SWC1900000001	Document Phase Final	Document Description ADDENDUM_1: RFP for Managed and Hosted Voice Services	Page 3 of 3
----------------------	--------------------------------	--	------------------------------

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions



Purchasing Division
 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 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:
 Pomeroy IT Solutions Sales Company, Inc. (dba Getronics)
 1020 Petersburg Road
 Hebron, KY 41048
 Robert Burlas, VP Sales South Central Region
 Phone: (317) 308-9060 / Email: Robert.Burlas@getronics.com

FOR INFORMATION CONTACT THE BUYER

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

Signature X *Robert Burlas* FEIN # 61-1352158 DATE Nov 15, 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).
3. To Publish revised Appendix_A document (rev. 10-24-2018).
4. To 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 VARIOUS LOCATIONS AS INDICATED BY ORDER		STATE OF WEST VIRGINIA 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

SWC1900000001	Document Phase Final	Document Description ADDENDUM_2: RFP for Managed and Hosted Voice Services	Page 3 of 3
----------------------	--------------------------------	--	------------------------------

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions



Purchasing Division
 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 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:

Pomeroy IT Solutions Sales Company, Inc. (dba Getronics)
 1020 Petersburg Road
 Hebron, KY 41048
 Robert Burlas, VP Sales South Central Region
 Phone: (317) 308-9060 / Email: Robert.Burlas@getronics.com

FOR INFORMATION CONTACT THE BUYER

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

Signature X *Robert Burlas*

FEIN # 61-1352158

DATE Nov 15, 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).

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 VARIOUS LOCATIONS AS INDICATED BY ORDER		STATE OF WEST VIRGINIA 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 #
51700			

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

SWC1900000001	Document Phase Final	Document Description ADDENDUM_3: RFP for Managed and Hosted Voice Services	Page 3 of 3
----------------------	--------------------------------	--	------------------------------

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions



Purchasing Division
 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 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:

PPomeroy IT Solutions Sales Company, Inc. (dba Getronics)

1020 Petersburg Road

Hebron, KY 41048

Robert Burlas, VP Sales South Central Region

Phone: (317) 308-9060 / Email: Robert.Burlas@getronics.com

FOR INFORMATION CONTACT THE BUYER

Mark A Atkins

(304) 558-2307

mark.a.atkins@wv.gov

Signature X

Robert Burlas

FEIN # 61-1352158

DATE Nov 15, 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.

o 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 VARIOUS LOCATIONS AS INDICATED BY ORDER		STATE OF WEST VIRGINIA 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: 4

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
- Attachment of vendor questions and responses
- Attachment of pre-bid sign-in sheet
- Attachment of Revised 11-15-2018 Attachment_A Cost Sheet
- Other

Description of Modification to Solicitation:

1. To Publish the Attachment_A Cost Sheets Revised 11-15-2018 due to calculation error.

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 Division
 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 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:

Pomeroy IT Solutions Sales Company, Inc. (dba Getronics)
 1020 Petersburg Road
 Hebron, KY 41048
 Robert Burlas, VP Sales South Central Region
 Phone: (317) 308-9060 / Email: Robert.Burlas@getronics.com

FOR INFORMATION CONTACT THE BUYER

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

Signature X *Robert Burlas* FEIN # 61-1352158 DATE Nov 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.

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 VARIOUS LOCATIONS AS INDICATED BY ORDER		STATE OF WEST VIRGINIA 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 #
1161700			

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

SOLICITATION NUMBER: CRFP 0212 SWC1900000001
Addendum Number: 5

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
- Attachment of vendor questions and responses
- Attachment of pre-bid sign-in sheet
- Attachment of Revised 11-16-2018 Attachment_A Cost Sheet
- Other

Description of Modification to Solicitation:

1. To move the Bid Opening date from 11/21/2018 to 11/27/2018 at 1:30pm EST.
2. To Publish the Attachment_A Cost Sheets Revised 11-16-2018 due to calculation error.

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.

	<p>Information Technology Department Policy Document</p>
---	--



Risk Assessment Policy

Version 18.2
June, 2018

History Log		
Version	Date	Author
Version 4.0	July 2016	Cameo Global-Eric A Walker
Version 4.1	Oct 2017	Jim Johnson
Version 4.2	Mar 2018	Jim Johnson
Version 18.2	June 2018	Approval – Andrew Higgins



Contents

1. Purpose.....3

2. Scope.....3

3. Policy.....3

ROLES & RESPONSIBILITY3

4. Reporting.....12

 Key Contacts.....12



1. Purpose

The purpose of this policy is to create a prescriptive set of process and procedures, aligned with applicable Cameo Global IT security policy and standards, to ensure Cameo Global develops, disseminates, and updates the Risk Assessment Policy.

2. Scope

This policy and procedure establishes the minimum requirements for the Cameo Global Risk Assessment Policy and is within scope for all Cameo Global employees.

3. Policy

Roles & Responsibility

This section will provide summary of the roles and responsibilities as described in the Statement of Policy section. The following Roles and Responsibility Matrix describe 4 activities:

- 1) Responsible (R) – Person working on activity
- 2) Accountable (A) – Person with decision authority and one who delegates the work
- 3) Consulted (C) – Key stakeholder or subject matter expert who should be included in decision or work activity
- 4) Informed (I) – Person who needs to know of decision or action



Information Technology Department Policy Document

Roles	Information Security Director	Department Head	Operations	Support	Information Security Board
Tasks					
CATEGORIZE AND DOCUMENT INFORMATION AND INFORMATION SYSTEMS.	I		A/R		C
INCLUDE THE SYSTEM CATEGORIZATION.	I		A/R		C
REVIEW THE SECURITY CATEGORIZATION ON AN ANNUAL BASIS.	I		A/R		C
CONDUCT AND DOCUMENT ASSESSMENT OF RISK.	I		A/R		C
REVIEW AND UPDATE RISK ASSESSMENT.	I		A/R		C
CREATE A RISK FINDING.	I		A/R		C
CREATE A RISK TREATMENT PLAN	I		A/R		C
SUBMIT A RISK ASSESSMENT PLAN AND RISK TREATMENT PLAN TO THE INFORMATION SECURITY DIRECTOR.	I	A			I
RECEIVE REPORTS FROM THE RISK REGISTER AND VERIFY IMPLEMENTATION.	I	A			I
VERIFY AND VALIDATE COMPLIANCE.	A				
SCAN AND ANALYZE INFORMATION SYSTEMS AND HOSTED APPLICATIONS FOR VULNERABILITIES.	I		A	R	R
REMEDiate VULNERABILITIES.	I		A	R	R
REVIEW AUDIT LOGS.	I		A	R	R
DOCUMENT VULNERABILITIES AND RISKS TO CAMEO SIB	I		A		I

A. SECURITY CATEGORIZATION



1. The Cameo Risk Assessment Policy requires that:
 - a. Information and the information systems must be categorized in accordance with Cameo policies and procedures;
 - i. The authorization boundary is a prerequisite and must be clearly defined before beginning the security categorization.
 - ii. Security categorization describes the potential adverse impacts to Cameo Global operations, assets, and individuals should the information and information system be comprised through a loss of confidentiality, integrity, or availability.
 - b. Security categorization results must be documented (including supporting rationale) in the Security Information Policy for the information system;
 - c. The security categorization must be conducted as a Cameo Global-wide activity;
 - i. Related staff, management, System Owner, and information security staff knowledgeable in the information created or collected by the program shall assist with the development of the security categorization.
 - d. Security categorization must be part of the system development life cycle (SDLC);
 - i. The security categorization must be reviewed and updated whenever there is a change in the information processed.
 - e. The security categorization must be reviewed at least on an annual basis; and
 - f. The security categorization decision must be reviewed and approved by the Vice President of Operations.
 - g. Security categories must be used in conjunction with vulnerability and threat information in assessing the risk to an organization resulting from the operation of its information systems.

B. RISK ASSESSMENT

1. The Vice President of Operations or designee must enforce the following Risk Assessment requirements for each IT system classified as sensitive to:
 - a. Identify potential threats to the confidentiality, integrity, and availability of an IT system and the environment in which it operates;
 - b. Determine the likelihood that threats will materialize;
 - c. Identify and evaluate vulnerabilities; and
 - d. Determine the loss impact if one or more vulnerabilities are exploited by a potential threat.



2. Risk assessments take into account vulnerabilities, threat sources, and security controls planned or in place to determine the level of residual risk posed to organizational operations and assets, individuals, other organizations, and the Cameo based on the operation of the information system.
 - a. Risk assessments also take into account risk posed to Cameo Global operations, Cameo Global assets, or individuals from external parties, including but not limited to:
 - i. Service providers.
 - ii. Contractors operating information systems on behalf of the organization.
 - iii. Individuals accessing Cameo Global information systems.
 - iv. Outsourcing entities.
 - v. Entities such as global clients and business competitors that may have an interested in information stored by CAMEO GLOBAL.
 - b. Risk assessments must be a collaborative effort among representatives of management, operational, technology and information security disciplines.
3. The System Owner shall:
 - a. Conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
 - i. The RA shall be conducted as needed, but not less than once every three years.
 - b. Document risk assessment results in a Risk Assessment Report, which includes, at a minimum, identification of all vulnerabilities discovered during the assessment, and an executive summary, including major findings and risk mitigation recommendations.
 - i. Updated reports must be sent to the Vice President of Operations.
 - c. Review risk assessment results at least once a year to determine the continued validity of the RA;
 - d. Update the risk assessment once a year or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system;
 - e. Use the results of the Cameo Global BIA and of the Data Classification procedure as primary inputs to the RA;
 - f. Create a risk finding for any risks identified in the risk assessment with a residual risk rating greater than a value of low; and



- g. Create a risk treatment plan for each risk assessment finding.
- 4. The Vice President of Operations or designee shall require that Cameo Global develop a risk assessment plan.
 - a. The Information Security Director shall submit the risk assessment plan to the Vice President of Operations on an annual basis.
 - b. The risk assessment plan must include the following:
 - i. The agency name, agency abbreviation and agency number,
 - ii. The contact information of individual submitting the plan,
 - iii. The date of submission,
 - iv. The system full name and abbreviation,
 - v. The planned assessor,
 - vi. The date the last risk assessment was conducted for the system, and
 - vii. Scheduled assessment completion date.

Note: Scheduled assessment completion date is the planned date of the completion of the future risk assessment covering a three year period from the submission date.

- 5. Until completion of all corrective actions in the risk assessment, the Information Security Director or designee shall receive reports, at least quarterly, from the risk register. The quarterly risk update will report progress toward implementing outstanding risk treatments.
- 6. Upon completion of the risk treatments shown in the risk register, Information Security Director or designee shall arrange for a follow-up review to verify implementation of the specified corrective actions.
- 7. The Information Security Director or designee shall submit to the Vice President of Operations the following information:
 - a. A record of all completed IT Risk Assessments conducted by or on behalf of Cameo.
 - b. Each risk identified in the risk assessment template must contain:
 - i. IT System Name
 - ii. Risk ID
 - iii. Sensitivity rating (e.g. Confidentiality, Integrity and availability)
 - iv. Date of risk assessment
 - v. Risk vulnerability family
 - vi. Vulnerabilities



- vii. Threats
 - viii. Risk Summary
 - ix. Magnitude of impact (e.g. low, moderate, high, critical)
 - x. Controls in place (brief description)
- c. For each risk identified, a Risk Treatment Plan must be submitted to the Vice President of Operations, and the plan shall include the:
- i. IT System affected
 - ii. Authoritative source
 - iii. Control ID
 - iv. Date risk identified
 - v. Risk summary
 - vi. Risk rating (Low, Med-Low, Med, Med-High, High, Critical)
 - vii. Status
 - viii. Status Date
 - ix. Planned resolution;
 - x. Resolution due date
- d. The Risk treatment plan for completed risk assessments must be submitted within 30 days of issuing the final risk assessment report. An updated risk treatment plan must be submitted quarterly (at the end of the quarter), until all resolutions are completed. All Risk Treatment Plans and quarterly updates submitted must have evidence of Information Security Director's approval.
8. The Cameo Global Information Director is responsible for verifying and validating compliance with the provisions of this policy and procedure.

C. VULNERABILITY SCANNING

1. The Risk Assessment Policy requires that:
- a. Information system and hosted applications must be scanned for vulnerabilities at least once every 90-days for publicly facing systems and sensitive information systems and when new vulnerabilities potentially affecting the system/applications are identified and reported;
 - i. The security categorization of the information system must guide the frequency and comprehensiveness of the vulnerability scans.



Information Technology Department Policy Document

- ii. Vulnerability analysis for custom software and applications may require additional, more specialized techniques and approaches (e.g., web-based application scanners, source code reviews, source code analyzers).
- iii. Vulnerability scanning must include scanning for specific functions, ports, protocols, and services that should not be accessible to users or devices and for improperly configured or incorrectly operating information flow mechanisms.
- iv. Cameo Global shall considers using tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to test for the presence of vulnerabilities.
- v. The following attributes, at a minimum, are required for vulnerability testing, as required by Cameo Global's Cameo Security and Risk Management, and are necessary to evaluate compliance for security certification and best practice adherence:
 1. Device Name,
 2. IP address,
 3. Device Type,
 4. Wireless Access Points,
 5. Description,
 6. OS Platform,
 7. Primary Admin,
 8. Location,
 9. Service Type,
 10. Service Port,
 11. Service Port Type,
 12. Application,
 13. Users of Service,
 14. Network Name,
 15. Network Type,
 16. Location Type,
 17. Location Access,
 18. Owning Location,



19. User Population Name and Type, and
 20. Primary User contact information (e.g. phone, email).
- b. Vulnerability scans must have defined a clear scope for all vulnerability scanning activities and designate knowledgeable and trained individuals to perform the scans. Prior to commencing vulnerability scanning efforts, the following should be addressed:
- i. Scanner selection – System Owners shall evaluate the tools for use within their respective environments.
 1. The network and host-based vulnerability scanner must provide the following capabilities:
 - i. Identify active hosts on networks.
 - ii. Identify active and vulnerable services (ports) on hosts.
 - iii. Identify vulnerabilities associated with discovered operating systems and applications.
 - ii. Scope/boundaries – An active vulnerability scan must have a defined scope or boundary. The scan must be limited to a specific information system, system(s), subnet(s), or network(s) within the realm of responsibility for CAMEO GLOBAL.
 1. Scans typically should be performed only on production systems and networks that are known to be stable and preferably during times of least impact to the critical functionality of the system. It is expected that vulnerability scanning will occur during various phases of the system's life cycle.
 - iii. Coordination/announcement – Coordination with and/or notification to the relevant or affected parties, depending on the scope and purpose of the scans, must occur before an active vulnerability scan is performed, especially if that scan may result in a potential negative impact.
 - c. The following must be addressed before and after the vulnerability scan:
 - i. Update scanning software – Before the vulnerability scan is performed, the vulnerability scanner must be updated with the latest patches and database signatures/tests. Scanners that are not maintained and out of date will not contain the most recent signatures/tests and, as a result, vulnerabilities could be missed.
 - ii. Verify system availability – After completing the test, the System Owner shall check system status directly or by coordinating with the system administration team to ensure that the test did not result in unintended consequences and that the system remains operational.



- d. Vulnerability scanning tools and techniques must be employed that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:
 - i. Enumerating platforms, software flaws, and improper configurations;
 - ii. Formatting and making transparent, checklists and test procedures; and
 - iii. Measuring vulnerability impact;
 - e. Vulnerability scan reports and results from security control assessments must be analyzed;
 - f. Vulnerabilities must be remediated within 90 days in accordance with an organizational assessment of risk; and
 - g. Information obtained from the vulnerability scanning process and security control assessments must be shared with designated personnel throughout the CAMEO GLOBAL to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).
2. The Vice President of Operations or designee shall enforce the following requirements:
- a. Vulnerability scanning tools must include the capability to readily update the list of information system vulnerabilities scanned.
 - b. The list of information system vulnerabilities scanned must be updated at least once every 90 days or when new vulnerabilities are identified and reported.
 - c. Vulnerability scanning procedures must be employed that can demonstrate the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).
 - d. Discerning what information about the information system is discoverable by adversaries must be attempted.
 - e. Privileged access authorization must be included for selected vulnerability scanning activities to facilitate more thorough scanning.
 - f. Historic audit logs must be reviewed to determine if a vulnerability identified in the information system has been previously exploited.
3. The Information Security Director shall document and report vulnerabilities and risks identified in the vulnerability scan and related remedial actions to CSRM once every 90 days.

Note: If no vulnerabilities were identified in a vulnerability scan, Agency must notify the Vice President of Operations that the vulnerability scan was conducted and there were no findings.

	<h1>Information Technology Department</h1> <h2>Policy Document</h2>
---	---

- a. Risks identified in Vulnerability scans must be reported to the Vice President of Operations using the Risk Assessment and Risk Treatment Plan templates and include the following information:
 - i. Date of Scan
 - ii. Host Name
 - iii. IP or DNS Entry
 - iv. Vulnerability description
 - v. Severity level/Risk Rating (high, medium, low)
 - vi. CVE #
 - vii. Remediation action (e.g. what's needed ... disable port, etc.)
 - viii. Results of follow-up scan after remediation action is taken

4. Reporting


Key Contacts

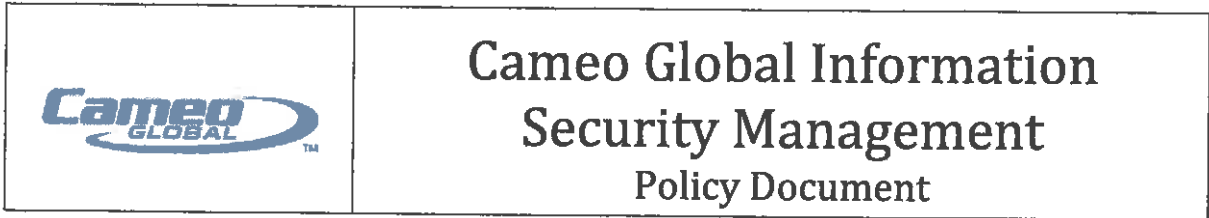
Cameo Global CloudBlu Information Security: Security@cameoglobal.com ;
ahiggins@cameoglobal.com, emichaud@cameoglobal.com, jjohnson@cameoglobal.com,
fwilliams@cameoglobal.com, mjackels@cameoglobal.com or toll free: 1-800-978-3163

Andrew Higgins, Vice President of Operations, is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above.

A current version of this document is available to all members of staff.

This policy is approved, as undersigned, by Andrew Higgins

DocuSigned by:
 Andrew Higgins Vice President operations 6/13/2018
Signature _____ Date _____



Cameo Global Information Security Policy

Version 18.4
October, 2018

History Log		
Version	Date	Author
Draft Version 4.0	Feb 2016	Eric A Walker
Final Version 4.1	March 2016	Nick Duncanson
Version 4.2	April 2016	NDuncanson / MHandermann/
Version 4.3	July 2016	Eric A Walker
Version 4.4	February 2017	Jim Johnson
Version 4.5	June 2017	Jim Johnson
Version 4.6	February 2018	Jim Johnson
Approval v18.2	June 2018	Andrew Higgins
Approval v18.4	October 2018	Andrew Higgins

	<h1 style="text-align: center;">Cameo Global Information Security Management Policy Document</h1>
---	---

Contents

1. Introduction	3
2. Information Security Policy Coverage.....	3
3. Policy Dissemination	3
4. Risk Assessment	4
5. Information Security Policy Review	4
6. Information Security Policy Responsibilities	4
7. Formal Security Awareness Program	4
8. Formal Acknowledgement Information Security Policies	5
9. Employee Screening and Background Checks.....	5
10. Third Party Service Provider Contractual Requirements	5
11. Connected Entity Requirements	5
12. Asset Classification.....	6
13. Roles and Responsibilities	8
14. User Access	11
15. User registration and de-registration (Creation & Deletion).....	11
16. Password Management	12
17. User Authentication	13
18. Review of access rights	13
19. Customer cardholder data Security	13



Cameo Global Information Security Management Policy Document

1. Introduction

This document provides the framework to develop and disseminate an information security policy in order to achieve common security compliance. This policy document is the master document, which is supported by other documents governing security compliance within Cameo Global.

2. Information Security Policy Coverage

Information Security Policy of the organization encompasses:

- Information Security Policy (this document)
- Access Control Policy
- Data Encryption Policy
- Data Retention, Retrieval and Secure Disposal Policy
- Human Resource Policy
- Change Management Policy
- Password management policy
- Network Security Policy
- Audit Log and Monitoring Policy
- Patch Management Policy
- Malicious Code Policy
- Vulnerability Management Policy
- Physical Access Control Policy
- Remote Access Policy
- Risk Assessment Methodology

3. Policy Dissemination

The information security policy must be published and disseminated to all relevant system users (including vendors, contractors, and business partners).



Cameo Global Information Security Management Policy Document

4. Risk Assessment

The Cameo Global organization will carry out an annual risk assessment process that would identify major strategic developments in the industry, emerging threats, & vulnerabilities to business and IT assets of the company and report results in a formal risk assessment document.

Standard Risk assessment methodologies can be considered which includes but not limited to OCTAVE, ISO 27005 and NIST SP 800-30.

5. Information Security Policy Review

The Cameo Global information security policy shall be reviewed at least quarterly and updated as needed to reflect changes to business objectives or the risk environment.

6. Information Security Policy Responsibilities

This Cameo Global information security policy Vice President of Operations Andrew Higgins as responsible for implementing and maintaining information security throughout the organization.

- Establish, document, and distribute security policies and procedures.
- Monitor and analyze security alerts and information, and distribute to appropriate personnel.
- Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.

Stakeholders:

1. Vice President of Operations – Andrew Higgins
2. Director of Global Operations – Everett Michaud
3. Business Compliance Manager-Jim Johnson



Cameo Global Information Security Management Policy Document

7. Formal Security Awareness Program

- ✓ Implement a formal security awareness program to make all employees aware of the importance of cardholder data security.
- ✓ Educate employees upon hire and at least annually (for example, by letters, posters, memos, meetings, and promotions).

8. Formal Acknowledgement Information Security Policies

Cameo Global requires employees to acknowledge in writing that they have read and understood the company's security policy and procedures.

9. Employee Screening and Background Checks

Cameo Global's current employees and the potential employees in the company would be screened through a defined procedure to minimize the risk of attacks from internal sources.

10. Third Party Service Provider Contractual Requirements

If cardholder data is shared with any of Cameo Global's third party service providers, then contractually the following is required:

- a) All contractual Cameo Global third party Service providers must adhere to the compliance requirements.
- b) Agreement including an acknowledgement that the contractual Cameo Global third party service provider is responsible for the security of cardholder data the provider possesses.

11. Connected Entity Requirements

All processors and Cameo Global's contractual third party service providers must maintain and implement policies and procedures to manage connected entities, to include the following:

- a) Maintain list of connected entities
- b) Ensure proper due diligence is conducted prior to connecting an entity.
- c) Ensure the entity has security compliance certificates, i.e. PCI, HIPPA, and SOC as examples.
- d) Connect and disconnect entities by following an established process.



Cameo Global Information Security Management Policy Document

12. Asset Classification

Data and information classification is the conscious decision to assign a level of sensitivity to data as it is being created, amended, enhanced, stored or transmitted. The classification of the data should determine the extent to which the data needs to be controlled/secured and is also indicative of its value in terms of Business Assets.

The term "Business Assets", for the purpose of the scope of this policy, refers to any information upon which the organization places a measurable value. By implication, the information is NOT in the public domain and would result in loss, damage or even business collapse, were the information to be lost, stolen, corrupted or in any way compromised.

Proper access controls and privilege levels are to be set before accessing sensitive cardholder data by any user internally. Media containing sensitive data shall only be distributed to the authorized in-house employees.

All applications and network hardware equipment which are accessible to the external parties and which transmit or deal with sensitive cardholder data should be protected by strong access control and authentication mechanisms.

Media containing sensitive data must not be handed over to any external entity or third party unless authorized by the management with proper business justification.

Cameo employees are required to adhere to 'Clean Desk' standards. This ensures that all sensitive and confidential information, whether on paper, storage media, or hardware is properly secured and protected from unauthorized view. Employees are prohibited from leaving Cameo private data or any customer data unattended or unsecured when the workstation is unoccupied.

- Computer workstations must be locked when the workstation is unoccupied.
- File cabinets or other physical storage containing sensitive or confidential information must be kept closed and locked when not in use or unattended.
- Passwords may not be written down in an accessible location.
- Printouts containing Restricted or Controlled information should be immediately removed from the printer.
- Documents containing sensitive or confidential information must be shredded upon disposal.
- Whiteboards containing sensitive or confidential information must be thoroughly erased.
- Storage devices when not in use such as CD's, DVD, hard drives, USB drives, etc. containing sensitive or confidential information must be secured in a drawer and data must be encrypted.
- Keys used to access sensitive or confidential information must be secured in a locked desk.



Cameo Global Information Security Management Policy Document

The following procedure should be followed for the purpose of data classification:

Computer output, regardless of media, which is classified in accordance with this classification scheme will be marked on the top and bottom of each page and/or on each output screen with the appropriate classification, except for the General classification, when it is created by the system.

12.1 General

This classification includes all information that may normally be considered as General information, however, for business reasons management has determined that its use and dissemination needs to be controlled.

Shredding of this information is not required for disposal.

12.2 Proprietary

All data and information, except for media releases approved by management, used in conducting day-to-day business is regarded as proprietary and is not intended for discussion or disclosure to other than Cameo Global staff.

Shredding of this information for disposal is desired but not required.

12.3 Restricted

Some of the data and information retained in the automated systems and on other media (e.g. microfiche, microfilm, and paper files) is critical to the continued profitability of the organization. Other data and information is regarded as personal since it pertains to our employees. To provide adequate protection for this type of material it will be given a classification level of Restricted for identification.

Shredding of this information for disposal is required.

12.4 Confidential

This category of information includes company plans, the premature release of which could be detrimental to the company's strategic plan (e.g. acquisitions being planned/negotiated) or which could result in the filing of civil or other litigation (e.g. release of additional stock for sale or a company buy back of outstanding stock). Also included in this category would be additional information specifically designated as secret by senior management.

This information is not authorized to be stored on any computer system except for desktop or laptop systems. When stored on desktop or laptop systems the information will be encrypted, using approved encryption software, to provide



Cameo Global Information Security Management Policy Document

adequate protection. Additionally, this information will not be transmitted over any computer network within or between Cameo Global's facilities unless it is encrypted, using approved encryption software.

If this information is stored on removable storage media, then such items should be properly identified and stored in a locked desk drawer, cabinet or safe when not in use.

Shredding of this information for disposal is required.

Guidelines for data classification and sensitivity must be documented and communicated to responsible data/information owners and all support personnel to ensure that information receives the appropriate level of protection.

13. Roles and Responsibilities

13.1 Vice President of Operations

Responsible for overseeing all aspects of information security, including but not limited to:

- ✓ Creating and distributing security policies and procedures
- ✓ Monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel
- ✓ Creating and distributing security incident response and escalation procedures that include:
 - Roles, responsibilities, and communication
 - Coverage and responses for all critical system components
 - Notification, at a minimum, of credit card associations and acquirers
 - Strategy for business continuity post compromise
 - Reference or inclusion of incident response procedures from card associations
 - Analysis of legal requirements for reporting compromises (for example, per California bill 1386)
- ✓ Annual testing
- ✓ Designation of personnel to monitor for intrusion detection, intrusion prevention, and file integrity monitoring alerts on a 24/7 basis



Cameo Global Information Security Management Policy Document

- ✓ Plans for periodic training
- ✓ A process for evolving the incident response plan according to lessons learned and in response to industry developments
- ✓ Maintaining a formal security awareness program for all employees that provides multiple methods of communicating awareness and educating employees (for example, posters, letters, meetings)
- ✓ Review security logs at least weekly and follow-up on exceptions



Cameo Global Information Security Management Policy Document

13.2 The Operations Department

Shall maintain daily administrative and technical operational security procedures that are consistent with the organization's compliance requirements that include:

- ✓ User account maintenance procedures
- ✓ Log review procedures

13.3 System and Application Administrators

- ✓ Monitor and analyze security alerts and information and distribute to appropriate personnel
- ✓ Administer user accounts and manage authentication
- ✓ Monitor and control all access to data
- ✓ Maintain a list of connected entities
- ✓ Perform due diligence prior to connecting an entity, with supporting documentation
- ✓ Verify that the entity is compliant with relevant compliance standards, with supporting documentation
- ✓ Establish a documented procedure for connecting and disconnecting entities
- ✓ Retain audit logs for at least one year

13.4 The Human Resources Office

Responsible for tracking employee participation in the security awareness program, including:

- ✓ Facilitating participation upon hire and at least annually
- ✓ Ensuring that employees acknowledge in writing that they have read and understand the company's information security policy
- ✓ Screen potential employees to minimize the risk of attacks from internal sources

13.5 Internal Audit

Shall be responsible for executing a risk assessment process that identifies threats, vulnerabilities and results in a formal risk assessment.



13.6 Contracts manager (or equivalent)

Ensure that for service providers with whom cardholder information is shared:

- ✓ Contracts require adherence to Cameo Global Inc. by all /any contractual third party service provider
- ✓ Contracts include acknowledgement or responsibility for the security of cardholder data by the service provider

14. User Access

14.1 Responsibilities

The Cameo Global Information Security team is responsible for creating, documenting and maintaining individual user/user group profiles that meet the requirements of Access Control Policy

14.2 Classification of users

Users are also classified in terms of:

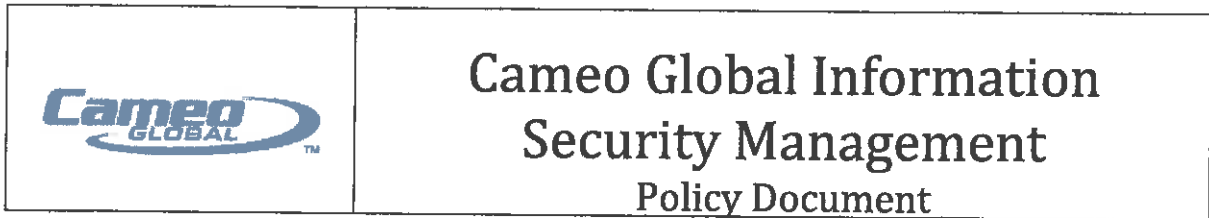
- The least number of privileges that are necessary to perform the job responsibilities
- Individual personnel's job classification and function

14.3 Privileges

Privileges are allocated on a need-to-use and event-by-event basis; the request for allocation of a privilege is initiated from the user concerned to the Cameo Global Information Security team which reviews the reasons why the privilege is required and the length of time for which it is required.

15. User registration and de-registration (Creation & Deletion)

User agreements contain statements of access rights and statements indicating that users have understood and accepted the conditions of access. Every user's proposed access rights are documented in a user form, which details the systems/services/applications/portals/information assets to which access is to be granted, together with the level of access that is granted, taking into account the *Access Control Policy*. If a user is to be granted access rights other than the standard ones set out in *Access Control Policy*, then the specific additional authorization of the



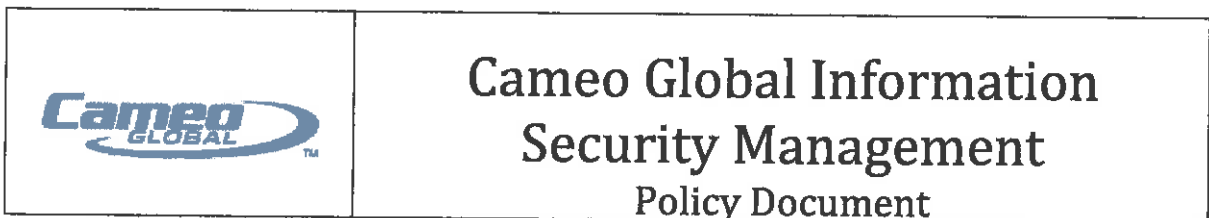
Management is also required.

- The Cameo Global Security team authorizes access to the system/asset and passes the User Creation/Deletion form to the Cameo Global Security officer and the user name/user ID is created/deleted and administered.
- The Cameo Global Security team maintains a list of authorized Users, administers changes in access rights and removes users.
- The disciplinary policy will be invoked in cases of attempted unauthorized access.

16. Password Management

The minimum password management requirements for the systems are as follows:

Requirement	Condition
Users to be issued with a temporary password, and to be forced to change on first login	○ Should be mandatory for Application Access for Individual Users – Internal and External
Password Expiry	○ Minimum of 90 days
Password length	○ Minimum of 7
Password complexity	○ Should be high and should contain at least one alphabet and one numeric character
Password history	○ Last 4 passwords
Period of Inactivity	○ Maximum of 90 days
Storage	○ Encrypted
Number of failed attempts for lockout	○ Maximum of 3
Lockout period	○ At least 30 minutes
Session Timeout	○ Maximum of 15 minutes of inactivity



Password State	<input type="radio"/> All local administrator accounts will accessed and stored using the Cameo Global Password State utility tool.
----------------	---

- First-time passwords for new users are set to a unique value for each user and MUST be changed after first use.
- The default passwords on all new equipment are changed to conform to Cameo Global Inc. Password Policy requirements before the equipment is brought into Production.

17. User Authentication


Users are authenticated at log-on by providing both their user name and their password within the parameters of the log-on system as per the section 6 of this document.

18. Review of access rights

- Access rights are reviewed by Cameo Global Information Security Team quarterly and their adequacy is confirmed.
- User access rights are reviewed when a user's role or location within organization changes in any way

19. Customer cardholder data Security

(Please ensure that you acknowledge in written agreement with customer confirming the customer's cardholder data in accordance with all applicable PCI requirements).

	<h1 style="text-align: center;">Cameo Global Information Security Management Policy Document</h1>
---	---

Cameo Global Inc. shall acknowledge in writing to all customers that the Cameo Global CloudBlu will maintain all applicable PCI DSS requirements to the extent the Cameo Global Inc. handles, has access to, or otherwise stores, processes, or transmits the customer's cardholder data or sensitive authentication data, or manages the customer's cardholder data environment on behalf of a customer.

Andrew Higgins, Vice President of Operations, is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above.

A current version of this document is available to all members of staff.

This policy is approved, as undersigned, by Andrew Higgins

<p><small>DocuSigned by:</small> <i>Andrew J Higgins</i> <small>B5C252816201711B...</small></p>	<p>10/29/2018</p>
<p>Signature</p>	<p>Date</p>



CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)
11/12/2018

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).

PRODUCER Willis of Minnesota, Inc. c/o 26 Century Blvd P.O. Box 305191 Nashville, TN 372305191 USA	CONTACT NAME: PHONE (A/C. No. Ext): 1-877-945-7378 FAX (A/C. No.): 1-888-467-2378 E-MAIL: certificates@willis.com ADDRESS:	
	INSURER(S) AFFORDING COVERAGE INSURER A: Great Northern Insurance Company INSURER B: Valley Forge Insurance Company INSURER C: Transportation Insurance Company INSURER D: INSURER E: INSURER F:	NAIC # 20303 20508 20494
INSURED Pomeroy IT Solutions, Inc. dba Getronics 1020 Petersburg Road Hebron, KY 41048		

COVERAGES **CERTIFICATE NUMBER:** W8831750 **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 SUBR INSD WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
A	<input checked="" type="checkbox"/> COMMERCIAL GENERAL LIABILITY <input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: <input checked="" type="checkbox"/> POLICY <input type="checkbox"/> PRO-JECT <input type="checkbox"/> LOC OTHER:	Y	3603-38-92 CIN	01/31/2018	01/31/2019	EACH OCCURRENCE	\$ 1,000,000
	DAMAGE TO RENTED PREMISES (Ea occurrence)					\$ 1,000,000	
						MED EXP (Any one person)	\$ 10,000
						PERSONAL & ADV INJURY	\$ 1,000,000
						GENERAL AGGREGATE	\$ 2,000,000
						PRODUCTS - COMP/OP AGG	\$ 2,000,000
							\$
A	<input checked="" type="checkbox"/> AUTOMOBILE LIABILITY <input checked="" type="checkbox"/> ANY AUTO <input type="checkbox"/> OWNED AUTOS ONLY <input type="checkbox"/> SCHEDULED AUTOS <input type="checkbox"/> HIRED AUTOS ONLY <input type="checkbox"/> NON-OWNED AUTOS ONLY <input type="checkbox"/> AUTOS ONLY		(17) 7359-18-78	01/31/2018	01/31/2019	COMBINED SINGLE LIMIT (Ea accident)	\$ 1,000,000
						BODILY INJURY (Per person)	\$
						BODILY INJURY (Per accident)	\$
						PROPERTY DAMAGE (Per accident)	\$
							\$
	<input type="checkbox"/> UMBRELLA LIAB <input type="checkbox"/> OCCUR <input type="checkbox"/> EXCESS LIAB <input type="checkbox"/> CLAIMS-MADE DED RETENTIONS					EACH OCCURRENCE	\$
						AGGREGATE	\$
							\$
B	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	N/A	WC 6 23661819	01/31/2018	01/31/2019	<input checked="" type="checkbox"/> PER STATUTE <input type="checkbox"/> OTH-ER	
	E.L. EACH ACCIDENT					\$ 1,000,000	
	E.L. DISEASE - EA EMPLOYEE					\$ 1,000,000	
C	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY PER STATUTE		WC 5 99732395	01/31/2018	01/31/2019	E.L. EACH ACCIDENT	\$1,000,000
						E.L. DISEASE - EA EMP	\$1,000,000
						E.L. DISEASE - POL LIM	\$1,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

SEE ATTACHED

CERTIFICATE HOLDER Office of Technology 00 Kanawha Blvd. E., Building 5, 10th Floor Charleston, WV 25305	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
---	--



ADDITIONAL REMARKS SCHEDULE

AGENCY Willis of Minnesota, Inc.		NAMED INSURED Pomeroy IT Solutions, Inc. dba Getronics 1020 Petersburg Road Hebron, KY 41048	
POLICY NUMBER See Page 1		EFFECTIVE DATE: See Page 1	
CARRIER See Page 1	NAIC CODE See Page 1		

ADDITIONAL REMARKS

THIS ADDITIONAL REMARKS FORM IS A SCHEDULE TO ACORD FORM,
 FORM NUMBER: 25 FORM TITLE: Certificate of Liability Insurance

Certificate Holder is included as an Additional Insured as respects to General Liability.

INSURER AFFORDING COVERAGE: Transportation Insurance Company NAIC#: 20494
 POLICY NUMBER: WC 6 23661836 EFF DATE: 01/31/2018 EXP DATE: 01/31/2019

TYPE OF INSURANCE:	LIMIT DESCRIPTION:	LIMIT AMOUNT:
WORKERS COMPENSATION AND EMPLOYERS' LIABILITY PER STATUTE	E.L. EACH ACCIDENT E.L. DISEASE - EA EMP E.L. DISEASE- POL LIM	\$1,000,000 \$1,000,000 \$1,000,000

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 exceeds 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: Pomeroy IT Solutions Sales Company, Inc. (d.b.a. Getronics)

Authorized Signature: Summer Bailey Date: 11/26/2018

State of West Virginia

County of Putnam, to-wit:

Taken, subscribed, and sworn to before me this 26 day of November, 2018.

My Commission expires Sept 25, 2019.

AFFIX SEAL HERE



NOTARY PUBLIC Nicole Rasnake

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.

West Virginia Ethics Commission
Disclosure of Interested Parties to Contracts

(Required by W. Va. Code § 6D-1-2)

Name of Contracting Business Entity: Getronics Address: 1020 Petersburg Road
Hebron KY 41048

Name of Authorized Agent: Summer Bailey Address: 135 Corporate Centre Drive, Suite 410 - Scott Depot, WV 25560

Contract Number: SWC1900000001 Contract Description: VOIP Hosted Services

Governmental agency awarding contract: West Virginia Dept. of Administration

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.

Cameo Global

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.

Nana Baffour-Gyewu & Franck Julien own Getronics.

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.

Robert Burlas, VP Sales Getronics

Signature: Summer Bailey
Robert Burlas

Date Signed: 11/26/2018

Notary Verification

State of WV, County of Putnam:

I, Robert Burlas, 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 26th day of November, 2018.

Nicole Rasnake
Notary Public's Signature

be completed by State Agency:
Date Received by State Agency: _____
Date submitted to Ethics Commission: _____
Governmental agency submitting Disclosure: _____

