Cisco Systems, Inc. Response to Request for Proposal

The State of Utah Division of Purchasing and General Services

WSCA-NASPO Master Agreement for Data Communications Products & Services

Solicitation JP14001

August 27, 2013

Cisco Systems, Inc. Response to Request for Proposal

The State of Utah Division of Purchasing and General Services

WSCA-NASPO Master Agreement for Data Communications Products & Services

Solicitation JP14001

August 27, 2013

Cisco Systems, Inc.

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134
HTTP://WWW.CISCO.COM

Cover Letter

August 27, 2013

Ms. Jennifer Porter
Purchasing Agent/Contract Analyst
1 State Office Building - Suite 3150
Salt Lake City, Utah 84114
Subject: Solicitation JP14001

Dear Ms. Porter:

Cisco Systems, Inc. is pleased to submit its technical and cost proposal through this transmittal letter to the State of Utah and WSCA-NASPO in response to the above-referenced Request for Proposal (RFP) for Data Communications Products & Services. Cisco is proud of its partnership with WSCA and the Participating States under our current WSCA Data Communications AR-233 contract since 2007. This rich experience has allowed us to fully understand and appreciate the WSCA-NASPO requirements under this RFP from both the OEM and end-user perspectives.

Cisco has successfully demonstrated that it is a trusted and reliable vendor and partner. We are tremendously proud of the impacts that we have made in helping our WSCA-NASPO government customers serve, protect, and improve the lives of its citizens and communities. For the past 5+ years, Cisco has provided its offerings to up to 19 Participating States and all the authorized users (local governments, schools, etc.) under those states. From Q1CY2008 – Q2CY2013, Cisco has sold over $679 million of its products and services under our current WSCA contract in partnership with 175 authorized resellers across the United States; and to date, we are pleased to have remitted $3.3 million in administrative fees to WSCA and $2.9 million total to those Participating States who also have their own administrative fees.

We believe that our response meets the requirements as called out in this State of Utah/WSCA-NASPO Solicitation JP14001, except as annotated in our response. If the State of Utah or WSCA-NASPO determines that Cisco's response is deficient in any way, Cisco respectfully requests to be promptly notified and be given the opportunity to correct any such deficiency. Please forward any questions regarding this solicitation response to me. My contact information is provided below.

On behalf of Cisco, thank you for giving us the opportunity to respond to this RFP and we look forward to continuing a mutually rewarding partnership.

Sincerely,

Mimi Nguyen
Sr. Manager, U.S. Public Sector Contracts Management Office
Office: 408.527.2627 I Cell: 650.228.8748 I Fax: 408.608.1802 I Email: mimnguye@cisco.com

Legal Disclaimer

Thank you for the opportunity to submit this non-binding (other than pricing for now-available products listed in our quotes) proposal for your consideration. Please note that this proposal may include proprietary, confidential, and/or trade secret information, which, if included, will be clearly marked as such in the proposal. Any information that Cisco considers to be a trade secret will not be subject to disclosure under any public records act.

Trademarks

Every effort has been made to identify trademark information in the accompanying text. However, this information may unintentionally have been omitted in referencing particular products. Product names that are not so noted may also be trademarks of their respective manufacturers.

Cisco is a registered trademark of Cisco Systems, Inc.

The Cisco logo is a registered trademark of Cisco Systems, Inc.

IOS is a registered trademark of Cisco Systems, Inc.

AnyConnect is a registered trademark of Cisco Systems, Inc.

CCIE is a registered trademark of Cisco Systems, Inc.

WebEx is a registered trademark of Cisco Systems, Inc.

IronPort is a registered trademark of Cisco Systems, Inc.

Meraki is a registered trademark of Cisco Systems, Inc.

Table of Contents

Cover Letter 1
Executive Summary 1
Why Cisco 2
Company Leadership and Global Workforce 2
Cisco Overview 2
Company Innovations 2
Cisco's Strength and Global Reach 2
Customer Satisfaction 3
Market leadership and Breadth and Depth of Technology Portfolio 4
Research and Development 5
Conclusion 5
Cisco Response to Point-by-Point Requirements 6
Appendix A — WSCA-NASPO Terms and Conditions with Noted Exceptions A-1
Appendix B — State of Utah Standard Information Technology Terms and Conditions with Noted Exceptions (For WSCA Contracts and DTS Related Contracts) B-1
Appendix C — Additional Vendor Terms and Conditions C-1
Exhibit A Glossary of Terms C-7
Acronyms 1

List of Figures

Figure 1. Cisco's Strength and Global Reach 2
Figure 2. Customer Satisfaction: A Cisco Priority 3
Figure 3. Market Leadership 4
Figure 4. Cisco Borderless Network Architecture 20
Figure 5. Cisco Collaboration Architecture 21
Figure 6. Cisco Unified Data Center 22
Figure 7. MDS 9124e FC Blade Switch for HP c-Class BladeSystem 76
Figure 8. MDS FC Blade Switch for IBM BladeCenter 76
Figure 9. Cisco Access Switch Benefits 79
Figure 10. Cisco's Professional Services Model 116

List of Tables

Table 1. Service Request Severity Definitions 25
Table 2. Automatic Email Alert Escalations for Cisco TAC Service Requests 25
Table 3. High-Level Implementation Roadmap 29
Table 4. Cisco WAAS Features and Benefits 40

List of Appendices

Appendix A —WSCA-NASPO Terms and Conditions with Noted Exceptions
Appendix B — State of Utah Standard Information Technology Terms and Conditions (For WSCA Contracts and DTS Related Contracts)
Appendix C — Additional Vendor Terms and Conditions

List of Attachments

Attachment 1, Cisco Cost Schedule

Legal Company Name (include d/b/a if applicable)	Federal Tax Identification Number	State of Utah Sales Tax ID Number
Cisco Systems, Inc.	77-0059951	VC0000118462

Ordering Address	City	State	Zip Code
To be provided once authorized resellers are selected for each Participating Addendum. This information will be posted on the required website. Same process as today.			

Remittance Address (if different from ordering address)	City	State	Zip Code
To be provided once authorized resellers are selected for each Participating Addendum. This information will be posted on the required website. Same process as today.			

Type Corporation ☐ Corporate Entity (not tax-exempt)	Company Contact Person Mimi Nguyen
Telephone Number (include area code) 408.527.2627 (office)	Fax Number (include area code) 408.608.1802
Companys Internet Web Address http://www.cisco.com	Email Address mimnguye@cisco.com
Discount Terms (for bid purposes, bid discounts less than 30 days will not be considered)	Days Required for Delivery After Receipt of Order (see attached for any required minimums)

The undersigned certifies that the goods or services offered are produced, mined, grown, manufactured, or performed in Utah. Yes No **X** . If no, enter where produced, etc.

We rely on contract manufacturers around the globe for substantially all of our manufacturing needs. We presently use a variety of independent third-party companies to provide services related to printed-circuit board assembly, in-circuit test, product repair, and product assembly. Proprietary software on electronically programmable memory chips is used to configure products that meet customer requirements and to maintain quality control and security. The manufacturing process enables us to

configure the hardware and software in unique combinations to meet a wide variety of individual customer requirements. The manufacturing process uses automated testing equipment and burn-in procedures, as well as comprehensive inspection, testing, and statistical process controls, which are designed to help ensure the quality and reliability of our products. The manufacturing processes and procedures are generally certified to International Organization for Standardization (ISO) 9001 or ISO 9003 standards.

Our arrangements with contract manufacturers generally provide for quality, cost, and delivery requirements; as well as manufacturing process terms, such as continuity of supply, inventory management, flexibility regarding capacity, quality, and cost management; oversight of manufacturing; and conditions for use of our intellectual property. We have not entered into any significant long-term contracts with any manufacturing service provider.

A downloadable Countries of Origin (COO) list will assist you with making the determination of which products are available from TAA-designated countries. This COO list is available to Cisco partners for download through the ordering tool and through Cisco Partner Central <http://www.cisco.com/web/partners/tools/country_of_origin.html>.

Offeror=s Authorized Representative=s Signature *See Original for Signature*	Date August 27, 2013
Type or Print Name Dana Giampetroni	Position or Title Director, Finance

Executive Summary

In a world that is changing quickly, it is essential that governments adopt new technologies and business models based on innovative governance methods and practices to improve public services for citizens. Collaboration, co-production across government sectors, and access to useable information from multiple sources are equally important in attaining these objectives. Government performance relies on innovation and technology to effectively run a "connected republic"—the next phase of e-government transformation where people and communities are at the center of new networks of knowledge, service, trust, and accountability. With our robust portfolio of advanced data communications/networking technologies and world-class offerings, Cisco Systems, Inc. (NASDAQ: CSCO) is committed to supporting Public Sector organizations to build their "Next Generation Networks" in order to meet the demands of their stakeholders in the 21st century. At Cisco, our customers come first and an integral part of our DNA is creating long-lasting partnerships and working with our customers to identify their needs and provide solutions that support their success.

Through market leadership, financial strength, and responsible business practices, we demonstrate our enduring capacity to serve the Public Sector as a key partner. We are helping cities, states, and nations manage through the major transitions that we are now facing together. This initiative will help our Public Sector organizations be more relevant to their constituents, enabling them to carry out their mission with a heightened effectiveness. For the Public Sector, we build on many years of understanding agency challenges and opportunities, and we respond by designing comprehensive solutions that address these issues. What does it mean to be a "Trusted Advisor" for the Public Sector? It means:

- Working closely with all agencies and listening to their unique service requirements
- Recognizing the power of using the "network as the platform" for integrated solutions building toward convergence
- Supporting agencies with capabilities that offer increased ROI by utilizing common infrastructure components (for example, Cisco video supporting next-generation learning and video; surveillance)
- Using the power of a connected network platform to introduce new capabilities such as energy, building, and transportation management
- Helping reduce costs and increase efficiency through virtualization
- Increasing citizen impact in discovering new ways of doing work through collaboration tools.

Why Cisco

Company Leadership and Global Workforce

With John Chambers as the CEO, Cisco employs a global workforce with technology centers across a wide range of locations, providing access to engineering talent throughout the world.

Cisco's global employee population is divided into four main segments, with about one-third of our employees in engineering, about one-third in sales, about one-sixth in services, and one-sixth in supporting groups. This workforce profile reflects Cisco's intense focus on delivering the right technology solutions to meet our customers' needs.

Cisco Overview

Quick Facts:

- Founded in 1984
- NASDAQ: CSCO
- FY 2013 Net Sales: $48.6 billion
- Q2 FY'13 Employee Count: 73,460.

Company Innovations

Cisco has been at the heart of many historic changes in technology, and that continues to be true today. Now, at a time when the technology industry is going through a period of dramatic change, Cisco is the market leader in multiple areas. The company helped catalyse the industry's move toward IP and, now that it is fully underway, the company is at the center of fundamental changes in the way the world communicates.

Cisco's Strength and Global Reach

Because of our Cisco family and ecosystem of partners, we've built a consistent track record of strength. We have the global reach our customers need to succeed in a shrinking world.

Figure 1. Cisco's Strength and Global Reach

We're pleased with our performance (Figure 1), which is among the best in the industry. And, as required for all public companies, our financial data undergoes rigorous accounting review to ensure our customers—and investors—have a full view into our financial status. We believe that we are on solid ground, which gives us business options that may not be available to companies in lesser financial positions. This provides risk mitigation for our customers, partners, and resellers.

Customer Satisfaction

In addition to our strength and global reach, we also have earned the trust and satisfaction of our customers. Each year, we hire a third-party research firm to survey thousands of Cisco customers worldwide. They are asked what we are doing well and where we need to improve.

Figure 2. Customer Satisfaction: A Cisco Priority

As you can see, since we began formally tracking this data, our numbers are strong. In 2012, we reached a possible customer satisfaction score 4.45 out of a possible 5.0. We believe that customers drive our company. And we also believe that we can never be "too close to a customer needs" or be "listening too much." It is through our customers that we identify and capture market transitions, measure our success, and design and create solutions. Our customer-centric approach—combined with our culture—is what makes us a "vendor of choice."

Market leadership and Breadth and Depth of Technology Portfolio

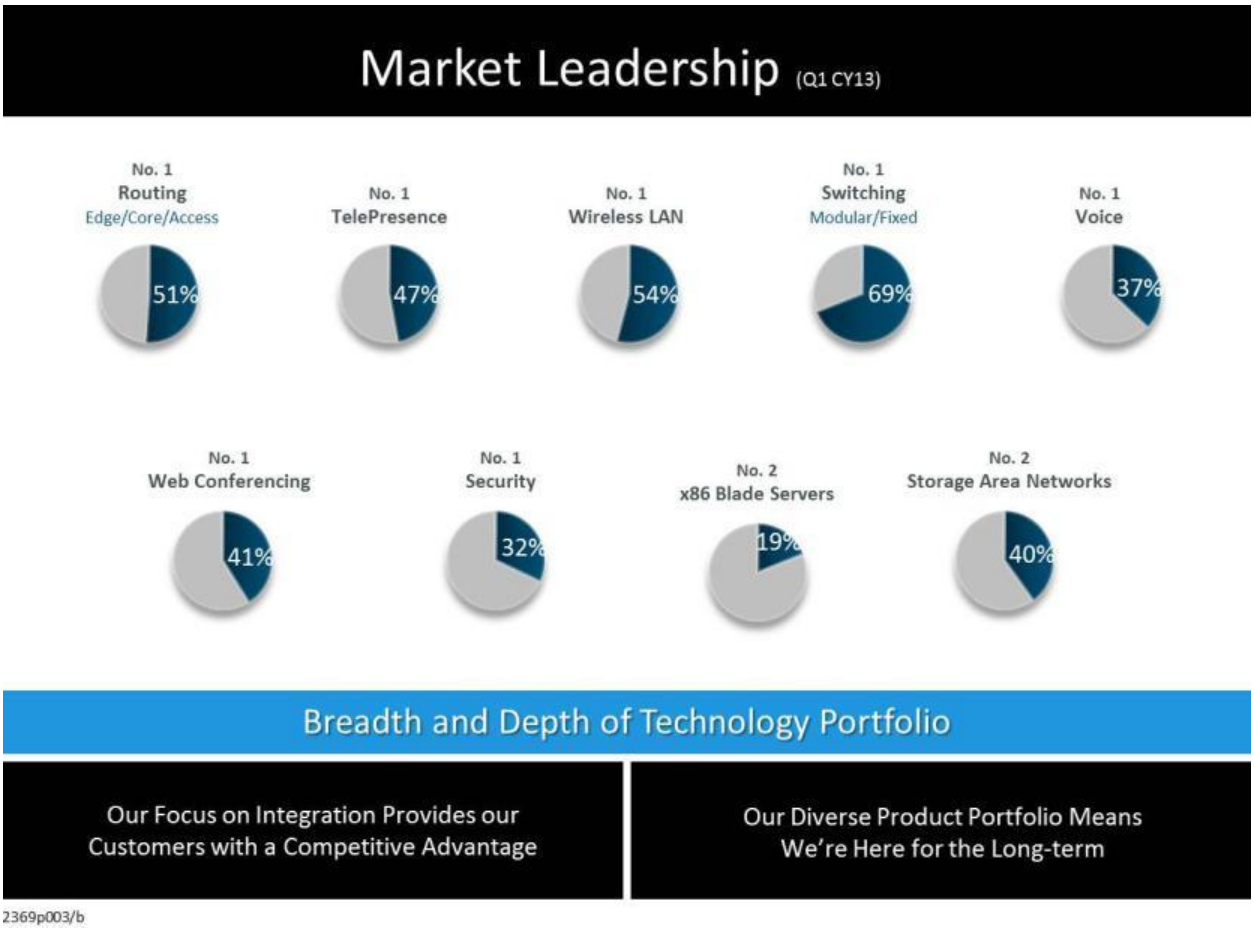

Figure 3. Market Leadership

Figure 3 depicts our market leadership and diverse product portfolio from collaboration to data center to cloud to security to Unified Computing. And this touches on just a few of our product categories—all of which we deliver as integrated architectures, enhancing the long-term stability of deployed solutions. We also offer a range of advanced, professional, and technical services covering these technologies and more. Our unmatched expertise in networking technology transitions makes us uniquely positioned to help customers capture the value of the Internet of Everything. Our ability to build, manage, and secure end-to-end IP-based platforms for people, process, data, and things will fuel the growth of the Internet of Everything. Only Cisco connects the unconnected with an open standard, integrated architecture from the cloud to end devices. Based on our rich history—and success in the market—connecting the previously unconnected is what we do best. We will continue to strive to be No. 1 in all of our markets.

Cisco is placed in the Leader's Quadrant of Gartner, Inc.'s 2012 Magic Quadrant for the following technologies:

- **Web Conferencing**
- **Corporate Telephony**
- **Unified Communications**
- **Contact Center Infrastructure Worldwide**

Research and Development

- Cisco spends more on R&D than anyone else in our industry — $5 billion per year.
- Cisco continuously tests product integrations and develops new innovative solutions through our R&D. Improvements are released through IOS updates, hardware upgrades, and new product rollouts.
- WSCA-NASPO customers can be assured that we leverage our assets to rapidly respond to changing market and technology requirements to support their needs.

Conclusion

Over the last several years, Cisco has built a strong, collaborative working relationship with WSCA-NASPO key business and technical stakeholders. Our primary goal has been to provide highly reliable, secure advanced networking products and support services to help the WSCA-NASPO customers protect, serve, connect, and educate more efficiently.

Cisco remains committed to creating networks and solutions that are smarter, thanks to built-in intelligent network services; faster, in their ability to perform at ever-increasing speeds; and more durable, with a generational approach to an evolutionary infrastructure. More specifically, Cisco supports Pubic Sector customers around the world by delivering innovative, integrated mission capabilities through thought leadership, advanced technologies, and services. The Cisco Public Sector staff comprises of a team of top experts from space, military, homeland security, and public safety from all levels of government around the world. They not only understand the unique challenges of government, but also bring years of personal experience to help solve these challenges.

Cisco Response to Point-by-Point Requirements

1.9 Governing Laws and Regulations

This procurement is conducted by the State of Utah, Division of Purchasing & General Services, in accordance with the Utah Procurement Code. These are available at the Internet website www.purchasing.utah.gov for the State of Utah's Division of Purchasing & General Services.

The laws of the State of Utah will govern all Master Agreements that result from this procurement unless the Data Communications Products and Services Provider and participating entity agree in a Participating Addendum that the laws of another jurisdiction will govern purchases made by purchasing entities within the jurisdiction of the participating entity.

Cisco Response:

Read and understood.

1.10 Length of Contract

The Master Agreement(s) resulting from this RFP will be for a period of five years (initial term). The Master Agreement(s) may be extended beyond the original Master Agreement period for a two (2) year period, by mutual agreement.

Cisco Response:

Read and understood.

1.11 Pricing Structure

Pricing Structure: Pricing for the WSCA-NASPO Master Agreements shall be based on the Percent Discount off the current global MSRP Schedule applicable to United States customers.

Cisco Response:

Read and understood. Cisco is pleased to offer the discounts off our entire U.S. Global Price Lists as set forth in the Cost Schedule. The discounts provided will remain valid for the contract term and will be applied to Cisco's then-current U.S. Global Price Lists.

The discounts provided are floor discounts (minimum guarantees) and individual transactions may qualify for additional, incremental discounts or incentives provided by Cisco's Authorized Resellers at their sole discretion. WSCA-NASPO, the Participating States and/or the Participating Entities may also actively solicit Cisco's Authorized Resellers for deeper discounts than the minimum contract pricing as set forth in the Cost Schedule. In any event, final transactional pricing shall be determined by the Authorized Resellers and not by Cisco; provided, however, that the minimum discounts set forth on the Cost Schedule are met.

The discounts on the Cost Schedule for new products are also applicable to Cisco's certified refurbished equipment. The price list for Cisco's certified refurbished equipment is separate from the U.S. Global Price Lists for new products, since they (i) are subject to inventory availability and (ii) are value priced considerably lower than equivalent new products.

1.12 Price Guarantee Period

Price Guarantee Period: The Data Communication Provider's Discount rate shall remain in effect for the term of the WSCA-NASPO Master Price Agreement.

Cisco Response:

Read and understood that the Discount Rates as set forth on Attachment 1 shall remain in effect for the term of the resulting WSCA-NASPO Contract.

1.13 Price Escalation

Equipment, Supplies and Services: Data Communications provider may update the pricing on their MSRP price list one time every year after the first year of the original contract term. The WSCA-NASPO Contract Administrator will review a documented request for a Price Schedule price list adjustment only after the Price Guarantee Period.

Cisco Response:

Cisco respectfully requests to take an exception to this Section 1.13. Because of the rapid pace of technological changes and advances, Cisco's entire U.S. Global Price Lists are refreshed on a monthly basis and made commercially available for our customers. To ensure that the Participating Entities have access to our then-current U.S. Global Price Lists, Cisco wishes to continue to provide monthly updates under the new WSCA-NASPO contract as well; provided, however, that the Discount Rates as set forth on Attachment C shall remain in effect for the entire term of the WSCA-NASPO Master Agreement. By providing the Participating Entities with monthly updates of Cisco's entire U.S. Global Price Lists, they can make smart and informed buying decisions based on the most up-to-date products and services options that are available to them.

1.14 Price Reductions

In the event of a price decrease in any category of product at any time during the contract in a Provider's Price Schedule, including renewal options, the WSCA-NASPO Contract Administrator shall be notified immediately. All Price Schedule price reductions shall be effective upon the notification provided to the WSCA-NASPO Master Agreement Administrator.

Cisco Response:

Cisco understands the importance of notifying the WSCA-NASPO Contract Administrator when there is a price decrease in Cisco's U.S. Global Price Lists for any of the awarded categories at any time during the contract term. However, given that Cisco is required to submit its updated U.S Global Price Lists to the WSCA-NASPO Contract Administrator as well as to the eMarket Center, Cisco respectfully requests that this Section 1.14 be revised to be consistent with Section 7.3.1 (3) whereby the "effective date" of such price reductions occurs when such updates are published in the e-Market Center. In addition, as stated earlier in Section 1.13, since Cisco's Price Lists are refreshed on a monthly basis that includes price reductions, Cisco wishes to provide updates on a monthly basis under the resulting WSCA-NASPO contract to ensure that Participating Entities will timely receive the benefits of such discounts.

1.15 Usage Reporting Requirement

All Data Communication Provider's will be required to provide quarterly usage reports to the WSCA-NASPO Contract Administrator or designee. The initiation and submission of the quarterly reports are the responsibility of the Data Communication Contract Provider. You are responsible to collect and report all sales data including your resellers and partners sales associated with your Master Agreement. There will be no prompting or notification provided by the WSCA-NASPO Contract Administrator.
Quarterly reports must coincide with the quarters in the fiscal year as outlined below:

Quarter #1: July 1 through September 30, due annually by October 30.
Quarter #2: October 1 through December 31, due annually by January 30.
Quarter #3: January 1 through March 31, due annually by April 30.
Quarter #4: April 1 through June 30, due annually by July 30.

Respondents must identify the person responsible for providing the mandatory usage reports. This contact information must be kept current during the Master Agreement period. The WSCA-NASPO Contract Administrator must be notified if the contact information changes. The contact information for the person responsible for the mandatory quarterly usage reporting must be specified per Section 3.1.5.

The purpose of the Master Agreement usage-reporting requirement is to aid in Master Agreement management. The specific report content, scope, and format requirements will be provided to the awarded Data Communications Products and Services Provider's during Master Agreement execution. Some WSCA-NASPO States may require additional reporting requirements. Those requirements will be addressed through the individual participating entity's Participating Addendum process. Failure to comply with this requirement may result in Master Agreement cancellation.

Cisco Response:

Cisco agrees to provide quarterly usage reports and proposes to use the same detailed reporting format template that it provides today under its current WSCA Data Communications AR-233 contract and to make the reports available to the WSCA-NASPO Contract Administrator and the Contractor Administrator of each Participating Entity who executed a Participating Addendum with Cisco via our web reporting tool at: https://pos.immixgroup.com/igcisco/. Cisco launched this tool to specifically support our current WSCA Data Communication AR-223 contract reporting obligations. We have received very positive feedback from numerous WSCA Contractor Administrators of the Participating States regarding its usefulness.

With respect to the quarterly report due dates for both the usage reports and administrative fee payments, Cisco respectfully requests an exception and proposes to keep the same due dates as set forth in Amendment #3 of the current Cisco WSCA Data Communications AR-233 contract, which are as follows:

Quarter #1:	July 1 through September 30, due annually by November 30.
Quarter #2:	October 1 through December 31, due annually by February 28.
Quarter #3:	January 1 through March 31, due annually by May 31.
Quarter #4:	April 1 through June 30, due annually by August 31.

Cisco requests additional time because as with the current WSCA Data Communications AR-233 contract, we anticipate that we will continue to have a robust list of subcontractors/resellers from whom we will need to collect quarterly usage reports.

1.16 Standard Contract Terms and Conditions

Any Master Agreement resulting from this RFP will include, but will not be limited to, the WSCA-NASPO Standard Master Agreement Terms and Conditions, the State of Utah Additional Terms and Conditions (Appendix A) and any additional terms and conditions specific to WSCA-NASPO participating addendums for participating entities. The WSCA-NASPO Master Agreement Terms and Conditions and State of Utah Additional Terms and Conditions will take highest precedence in any contract resulting from this solicitation. Vendors must clearly identify exceptions to the WSCA-NASPO Standard Master Agreement Terms and Conditions and the State of Utah Additional Terms and Conditions in the bid submission. Vendor exceptions must include proposed solution language. Failure to submit exceptions and/or solution language will constitute vendor acceptance of WSCA-NASPO and State of Utah Additional Terms and Conditions. No third party terms and conditions will be allowed in resulting contracts awarded under this solicitation. Additional vendor terms and conditions must be submitted with the solicitation bid response for legal review and contract applicability. Submission of vendor terms and conditions with a bid response does not guarantee acceptance. Vendor terms and condition will not include any reference to website URLs that house additional terms and conditions. All terms and conditions associated with resulting contracts will be identified and attached to the WSCA-NASPO Master Agreement. The State of Utah reserves the right to accept, reject, and/or negotiate vendor terms and conditions after the award(s) have been made if it is in the best interest of the State of Utah. Participating States reserve the right to negotiate vendor terms and conditions during the Participating Addendum process. Vendor terms and conditions included with a bid response are limited to a maximum of 10 pages ($8^{1/2}$ x 11 inch paper, 10 pt Arial font, and single sided). Failure to adhere to these terms and conditions requirements may result in vendor disqualification.

Cisco Response:

WSCA-NASPO Standard Master Agreement Terms and Condition exceptions can be found in Appendix A. State of Utah Standard Information Technology Terms and Conditions exceptions can be found in Appendix B, and Additional Vendor terms and conditions can be found in Appendix C.

1.17 Questions

All questions must be submitted through BidSync. Answers will be given via the BidSync website. Questions received after the Question/Answer period will not be answered. No agency employee, board member, or evaluation committee member should be contacted concerning this solicitation during the solicitation posting and selection process. Failure to comply with this requirement may result in vendor disqualification.

Cisco Response:

Read and understood.

1.18 Discussions with Respondents (Oral Presentation)

An oral presentation by a Respondent to clarify a proposal may be required at the sole discretion of the WSCA-NASPO Master Agreement Administrator. However, the WSCA-NASPO Contract Administrator may award a Master Agreement based on the initial proposals received without discussion with the Respondent. If oral presentations are required, they will be scheduled after the submission of proposals. Oral presentations will be made at the Respondents expense.

Cisco Response:

Read and understood. Cisco welcomes the opportunity, at its sole expense, to provide an oral presentation to clarify on its bid response.

1.19 Protected Information

The Government Records Access and Management Act (GRAMA), Utah Code Ann., Subsection 63-2-304, provides in part that:

> the following records are protected if properly classified by a government entity:
> (1) trade secrets as defined in Section 13-24-2 if the person submitting the trade secret has provided the governmental entity with the information specified in Section 63-2-308 (Business Confidentiality Claims);
> (2) commercial information or non-individual financial information obtained from a person if:
> (a) disclosure of the information could reasonably be expected to result in unfair competitive injury to the person submitting the information or would impair the ability of the governmental entity to obtain necessary information in the future;
> (b) the person submitting the information has a greater interest in prohibiting access than the public in obtaining access; and
> (c) the person submitting the information has provided the governmental entity with the information specified in Section 63-2-308;
> * * * * *
> (6) records the disclosure of which would impair governmental procurement proceedings or give an unfair advantage to any person proposing to enter into a contract or agreement with a governmental entity, except that this Subsection (6) does not restrict the right of a person to see bids submitted to or by a governmental entity after bidding has closed; ....

GRAMA provides that trade secrets, commercial information or non-individual financial information may be protected by submitting a Claim of Business Confidentiality.

To protect information under a Claim of Business Confidentiality, the Respondent must:

1. provide a written Claim of Business Confidentiality at the time the information (proposal) is provided to the State, and
2. include a concise statement of reasons supporting the claim of business confidentiality (Subsection 63-2-308(1)).
3. submit an electronic "redacted" (excluding protected information) copy of your proposal response. Copy must clearly be marked "Redacted Version." Failure to submit a redacted version may result in release of your entire proposal.

A Claim of Business Confidentiality may be appropriate for information such as client lists and non-public financial statements. **Pricing and service elements cannot be protected**. **An entire proposal cannot be protected under a Claim of Business Confidentiality or Propritary. Failure to comply with this requirement many result in your proposal being ruled Non-Responsive** and no longer considered**.** The claim of business confidentiality must be submitted with your proposal on the form which may be accessed at:

www.purchasing.utah.gov/contract/documents/confidentialityclaimform.doc

To ensure the information is protected, the Division of Purchasing asks the Respondent to clearly identify in the Executive Summary and in the body of the proposal any specific information for which a Respondent claims business confidentiality protection as "PROTECTED".

All materials submitted become the property of the State of Utah. Materials may be evaluated by anyone designated by the State as part of the sourcing team. Materials submitted may be returned only at the State's option.

Cisco Response:

Read and understood. No confidential material has been included as part of this response.

1.20 WSCA Administrative Fee

The Contracted Supplier must pay a WSCA-NASPO administrative fee of one quarter of one percent (.025%) in accordance with the terms and conditions of the contract. The WSCA-NASPO administrative fee shall be submitted quarterly and is based on the actual sales of all products and services in conjunction with your quarterly reports. The WSCA-NASPO administrative fee must be included when determining the pricing offered. The WSCA-NASPO administrative fee is not negotiable and shall not be added as a separate line item on an invoice.

Additionally, some WSCA-NASPO participating entities may require that an administrative fee be paid directly to the WSCA-NASPO participating entity on purchases made by purchasing entities within that State. For all such requests, the fee percentage, payment method and payment schedule for the participating entity's administrative fee will be incorporated in the Participating Addendum. Data Communications Provider will be held harmless, and may adjust (increase) the WSCA-NASPO Master Agreement pricing by the fee percentage for that participating entity accordingly for purchases made by purchasing entities within the jurisdiction of the State. All such agreements may not affect the WSCA-NASPO fee or the prices paid by the purchasing entities outside the jurisdiction of the participating entities requesting the additional fee.

Cisco Response:

Cisco agrees to pay the WSCA-NASPO administrative fee of one quarter of one percent (.25%) based on actual sales of all products and services as shown on the quarterly usage reports. For purposes of clarification, Cisco understands "actual sales" to mean net purchase price, which is Cisco's product list price, minus all applicable contract discounts, rebates or vale added incentives, and excluding sales, use or other applicable taxes, surcharges or like fees, to the extent applicable to an order. This definition is consistent with the language in Cisco's current WSCA Data Communications AR-233 contract as set forth in Section D3, Attachment A. In addition, Cisco respectfully requests an exception that the remittance due

dates for the administrative fees to be the same as the current due dates as set forth in Amendment #3 of the current WSCA Data Communications AR-233 contract, which are as follows:

Quarter #1:	July 1 through September 30, due annually by November 30.
Quarter #2:	October 1 through December 31, due annually by February 28.
Quarter #3:	January 1 through March 31, due annually by May 31.
Quarter #4:	April 1 through June 30, due annually by August 31.

These are the same deadlines we are also requesting for the quarterly usage reports as set forth in our response to Section 1.15 above.

In the event WSCA-NASPO changes the administrative fee (increase or decrease), Cisco is respectfully requesting that at least a sixty (60) days advance notice of such change in order for Cisco to implement the new administrative fee accordingly internally and with its Authorized Resellers.

1.21 Interest

Any payments that a Contracted Supplier makes or causes to be made to WSCA-NASPO after the due date as indicated on the Quarterly Report schedule shall accrue interest at a rate of 18% per annum or the maximum rate permitted by law, whichever is less, until such overdue amount shall have been paid in full. The right to interest on late payments shall not preclude WSCA-NASPO from exercising any of its other rights or remedies pursuant to this agreement or otherwise with regards to Data Communication Provider's failure to make timely remittances.

Cisco Response:

Cisco takes exception to this section and respectfully requests that any sum not paid when due shall bear interest until paid at a rate of 1% percent per month (12% per annum) or the maximum legal rate, whichever is less. This definition is consistent with the late fees due to Cisco from a purchaser under the proposed current WSCA Data Communications AR-233 contract and proposed WSCA-NASPO Master Agreement Terms and Conditions (Section 22).

1.22 Proposal Offer Firm

Responses to this RFP, including proposed discounts offered will be considered firm for one hundred and sixty (160) days after the proposal due date. By signature (electronic or otherwise) and submission of a proposal, the person signing verifies that they are authorized to submit the proposal and bind the firm to provide the products/services in the proposal and potential Master Agreement.

Cisco Response:

Read and understood.

1.23 Cancellation of Procurement

This RFP may be canceled at any time and any and all proposals may be rejected in whole or in part when the State of Utah, Division of Purchasing and General Services determines such action to be in the best interest of the State of Utah.

Cisco Response:

Read and understood.

1.24 Right to Waive

The sourcing team reserves the right to waive minor irregularities at its sole discretion.

Cisco Response:

Read and understood.

1.25 Right to Accept All or Portion

It is our intent to accept the entire line of Data Communications Equipment and Services (included in the scope) from the awarded Data Communications Providers, however we reserve the right to accept all or a portion of a Respondents proposal.

Cisco Response:

Read and understood.

1.26 Service Line Additions and Updates

During the term of the contract, Data Communications Providers may submit a request to update the awarded items (within the scope listed in IDENTIFY SECTION) as new technology is introduced, updated or removed from the market. The Master Agreement Administrator will evaluate requests and update the contract offering via written amendment as appropriate. The Data Communications Service Provider shall update the dedicated website, price lists, and catalogs to reflect approved changes. Pricing must utilize the same pricing structure as was used for services falling into the same service category.

Cisco Response:

Read and understood that this Section 1.26 applies to both awarded products and services offerings and not just "service" items as set forth in the header of this section. In addition, as stated in Section 1.12 above, since Cisco's U.S. Global Price Lists are updated on a monthly basis , we would appreciate the ability to submit updated pricebooks for the awarded items on a monthly basis as well.

1.27 Right to Publish

Throughout the duration of this procurement process and Master Agreement term, Respondents, Data Communications Providers and their authorized contractors must secure from the WSCA-NASPO Contract Administrator prior approval for the release of any information that pertains to the potential work or activities covered by this procurement or the Master Agreement. The Data Communications Provider shall not make any representations of WSCA-NASPO's opinion or position as to the quality or effectiveness of the services that are the subject of this Master Agreement without prior written consent of the WSCA-NASPO Contract Administrator. Failure to adhere to this requirement may result in disqualification of the Respondents proposal or termination of the Master Agreement for cause

Cisco Response:

Read and understood.

1.28 Changes in Representation

The Contracted Supplier must notify the WSCA-NASPO Contract Administrator of changes in the Contracted Supplier's key administrative personnel, to the extent that there may be adverse impacts to the contract. The WSCA-NASPO Contact Administrator reserves the right to require a change in Contracted Supplier(s) representatives if the assigned representative(s) is not, in the opinion of the WSCA-NASPO Contract Administrator, meeting the terms and conditions of the contract.

Cisco Response:

Read and understood.

1.29 E-Rate Requirement

All award contractors must commit to participation in the Federal Communication Commission's E-rate discount program established under authority of the Federal Telecommunications Commission Act of 1996. Participation in, and implementation of, this program must be provided without the addition of any service or administration fee by the contractor.

Cisco Response:

Read and understood.

1.30 Section 508 Compliant

Respondents must meet all Federal and State regulations required to these type of products including but limited to accessible products by describing their support of the applicable provisions of the Workforce Investment Act of 1998, Section 508.

Cisco Response:

Cisco is a key contributor to accessibility standards and guidelines created by the International Telecommunications Union (ITU), the Internet Engineering Task Force (IETF), the Telecommunications Industry Association (TIA), and others. Cisco operates in a spirit of openness, as demonstrated by its participation in virtually every industry group concerned with networking standards and in its willingness to share innovations with others.

Cisco Accessibility Policy

The following key objectives for company business processes and activities help ensure that Cisco products and services benefit the disabled community:

- Increase awareness of accessibility within Cisco
- Provide employees with the training needed to design, produce, market, and deliver accessible products, websites, and documentation
- Develop and apply policies and guidelines to evaluate accessibility, usability, and compatibility with applicable equipment, services, websites, and documentation
- Evaluate accessibility and usability throughout the product design, development, and fabrication processes as early and consistently as possible
- Report ways these guidelines are implemented where competitively, technically, and economically feasible
- Involve people with disabilities in research projects, testing, and trials
- Support and contribute to industry standards and guidelines for accessibility.

Cisco and Accessibility Standards Section 508 of the Rehabilitation Act

Cisco complies with accessibility laws, and strives to supply end-user devices that conform and support the U.S. Access Board's standards as referenced in Section 508 of the Rehabilitation Act.

Section 255 of the Telecommunications Act

Cisco employs common accessibility features in its user devices, documents, and services, and has tested and achieved compatibility with third-party assistive devices. Its networks are compatible with common analog devices from the network core to the individual user.

Americans with Disabilities Act

Cisco complies with the ADA by enabling accessibility and accommodation in public areas and its customers' workplaces, and by implementing reasonable accommodation in its own workplace.

The 21st Century Communications and Video Accessibility Act

The CCVA is divided into two broad titles or sections. Title I addresses communications access to make products and services using broadband fully accessible to people with disabilities. Title II of the accessibility act breaks new ground to make it easier for people with disabilities to view video programming on television and the Internet. Cisco is participating in the review of these new requirements and researching the applicability to Cisco products.

World Wide Web WCAG 2.0 (Web Content Accessibility Guidelines)

In June 2009, Cisco adopted the WCAG 2.0 Level A requirements as best practices for development, testing, and overall conformance for the Accessibility of Cisco Web-based products.

Standards

Cisco accessibility initiatives are based soundly on public standards, including those issued by the U.S. Access Board; and on guidelines, including those published by the international World Wide Web Consortium.

1.31 Glossary

Authorized Contractor: The Prime Contractor as listed as Contractor under the resulting Master Agreement(s) as a result of this RFP.

Authorized Sub Contractor: Sub Contractor, Reseller, Partner, etc. Authorized by the Contractor (Prime) to sell only the products and services listed under the Master Agreement (s) established as a result of this RFP. This authorized sub contractor must have the authority and ability to accurately reflect the ability of the Respondent to meet the requirements detailed in this RFP.

WSCA-NASPO Contract Administrator: A dedicated person with the authority and ability to manage compliance with the scope and terms and conditions for this contract.

Mandatory Minimum Requirements: Requirements that must be met in order to be considered for further evaluation. Mandatory minimum requirements are non-negotiable. An offer that does not meet the mandatory minimum requirements will be disqualified from further consideration.

Participating Addendum: A Participating Addendum must be executed by any State that decides to adopt a WSCA-NASPO Master Agreement.

A Participating Addendum shall be executed for each contractor by the individual State desiring to use their contract.

Additional States may be added with the consent of the contractor and the Lead State (on behalf of WSCA-NASPO) through execution of Participating Addendums.

A Participating Addendum allows for each Participating State to add terms and conditions that may be unique to their State.

The Participating State and the Contractor shall negotiate and agree upon any additional terms and conditions prior to the signing and execution of the Participating Addendum.

States are not mandated to sign a Participating Addendum with all awarded vendors.

Participating Entity: A State that has indicated intent to participate in the solicitation process, or after award, a State that has executed a participating addendum.

Purchasing Entity: Any end-user in a Participating State that is eligible to use the Master Agreement(s) through the Participating Addendum, including but not limited to State Agencies, Counties, Cities, Education, and other entities.

Qualified Entity: An entity that is eligible to use the Master Agreement(s).

Usage Report Administrator: A contractors person responsible for the quarterly sales reporting and payments described in Section 1.15 Usage Reporting Requirement.

Volume Discount: A percentage discount offered by the seller to the buyer for purchasing a stated dollar amount of Data Communications services and products to be delivered at one time or for a specified period.

Sourcing Team: The technical and business team charged with setting requirements for the Data Communications procurement, and its subsequent evaluation.

Cisco Response:

Read and understood.

Section 2: General Proposal Requirements and Information

2.1 Proposal Content and Format Requirements

Proposals must be detailed and concise. Unless otherwise stated in your proposal as an "exception", Respondents agree to comply with every section, subsection, attachment and addendum of this RFP. Each proposal must be submitted in Microsoft Word or Excel, labeled and organized in a manner that is congruent with the section number, headings, requirements, and terminology used in this RFP. Proposal documents must be Arial font size 10. Respondent responses that are limited to a specified number of pages are referring to single sided pages. As an example, a response that is limited to a document that is no more than two pages long may be submitted on one double sided page, but not two double sided pages.

Cisco Response:

Read and understood.

2.2 RFP Revisions

Revisions, if any, and all written questions and the State's answers, will be posted on the BidSync website. Solicitation documents will not be mailed to prospective Proposers. Respondents must register (free of charge) as a vendor with BidSync in order to have access to the RFP and related documents. Respondents are responsible for ensuring that their registration information is current and correct. The State of Utah accepts no responsibility for missing or incorrect information contained in the supplier's registration information on BidSync. The State of Utah accepts no responsibility for a prospective Respondent not receiving solicitation documents and/or revisions to the solicitation. It is the responsibility of the prospective Respondent to obtain the information provided through BidSync.

Cisco Response:

Read and understood.

2.3 Right to Waive

The State of Utah reserves the right to waive any informality or technicality in any proposal.

Cisco Response:

Read and understood.

2.4 Proposals Become Property of the State of Utah

All proposal contents become the property of the State of Utah. All proposal content is proprietary during the proposal evaluation process. Upon Master Agreement award, the successful Respondents' proposals will be open to public inspection, by request, with the exception of any proposal content that is marked as "proprietary or confidential" by the Respondent. All content designated as "proprietary or confidential" must be supported by documentation as to the rationale for the proprietary nature of the information.

Cisco Response:

Read and understood.

2.5 News Releases

News releases or other public disclosure of information pertaining to this RFP or the statewide contracts may not be published without the prior written permission of the State of Utah.

Cisco Response:

Read and understood.

2.6 State Seal Use

The Utah GREAT SEAL RULE states, in section R622-2-3.Custody and Use, that “no facsimile or reproduction of the Great Seal may be manufactured, used, displayed, or otherwise employed by anyone without the written approval of the Lieutenant Governor."

Other participating States have similar rules that must be adhered to by Respondents or interested parties.

Cisco Response:

Read and understood.

Section 3: Data Communications Provider Mandatory Minimum Requirements

3.1 General Information

This section contains requirements that must be addressed in order for your proposal to be considered for the evaluation phase of this RFP. All of the items described in this section are non-negotiable. Respondents are required to complete:

Mandatory Requirements (M)

All Respondents must meet the **(M)** requirements listed in this section, and explain how the requirement is met. A ‘no’ response on the acceptance document or omission of the required explanation will disqualify the service from further evaluation.

3.1.1 Equipment Offering

(M) Identify Equipment Offering in sections 5.2.1-5.3.0.

Cisco Response:

Cisco is offering our entire U.S. Global Price Lists (GPLs) in response to this RFP. Cisco product lines extend to several hundred individual products. These products are developed by and organized into integrated architectures, providing a seamless approach to presenting solutions for organizations’ technology needs. We feel that our broad portfolio of products meets the requirements for every product category as set forth in Section 5.2.1 – 5.3 and in the Cost Schedule.

Cisco’s products are generally integrated into solutions or architectures for a majority of technology categories listed in this RFP. Server products and associated software are integral components of many of these networking solutions and architectures. These solutions simply cannot not be implemented, nor meet our customers’ basic operational expectations and requirements, without the included server components. Therefore, Cisco is offering server products and software as part of our integrated solutions where required, but not as a separate stand-alone product category. For example, regarding our collaboration portfolio, Cisco Unified Computing System (USC) servers run Cisco Call Manager software, which drives our enterprise telephony platform. Likewise, our Unity products (voice mail) and our E911 solution are driven by UCS servers. Turning to network security, our servers drive the Cisco Identity Services Engine (ISE) software which is a key component of our security portfolio. Similarly, with regard to network management, our UCS servers host the components that make up the Cisco Prime LAN Management System, including Cisco Prime Network Control System, Cisco Prime Infrastructure, and Cisco Prime Security Manager. It should also be noted that not only do our servers run and drive these

solutions they also unify computing, networking, management, virtualization, and storage access into a single integrated architecture that enables end-to-end server visibility, management, and control, thereby enhancing our customers' ability to effectively, efficiently, and economically serve their constituents.

3.1.2 Service Offering

(M) Identify Service Offerings for all products offered in Sections 5.2.1-5.3.0.

Cisco Response:

For each of the offerings listed in 5.2.1 – 5.3.0, Cisco and our resellers offer a comprehensive family of IT services. Regardless of the technology that a customer is deploying, Cisco's holistic services approach provides customers with the necessary tools to analyze and implement technology during every portion of their IT lifecycle. From the planning phase, to building phase, to the managing phase, customers can rely on Cisco services.

Cisco is pleased to offer its full portfolio of technical/maintenance services and or professional/advanced services. Our service model is designed to allow customers to leverage Cisco services for their specific technology no matter where they are on the IT lifecycle.

A detailed description of Cisco's services portfolio is provided under sections 5.3.1.1 and 5.3.1.2.

3.1.3 Insurance Requirement

(M) This pertains to the State of Utah insurance requirements. Other Participating States may identify different insurance requirements during the participating addendum process.

Data Communications Provider's and their authorized contractors shall procure and maintain insurance which shall protect the authorized contractor and The State and/or purchasing entity (as an additional insured) from any claims from bodily injury, property damage, or personal injury covered by the indemnification obligations set forth herein. The Data Communications Provider's authorized contractor shall procure and maintain the insurance policies described below at their own expense and shall furnish to the procurement manager, upon award, an insurance certificate listing the participating State(s) as certificate holder and as an additional insured. The insurance certificate must document that the Commercial General Liability insurance coverage purchased by the authorized contractor to include contractual liability coverage applicable to this Master Agreement. In addition, the insurance certificate must provide the following information: the name and address of the insured; name, address, telephone number and signature of the authorized agent; name of the insurance company (authorized to operate in all States); a description of coverage in detailed standard terminology (including policy period, policy number, limits of liability, exclusions and endorsements) and an acknowledgment of notice of cancellation to the participating States.

> Authorized contractor is required to maintain the following insurance coverage's during the term of the WSCA-NASPO Master Agreement:
>
> 1) Workers' Compensation Insurance – The Data Communications Provider's authorized contractor must comply with Participating State's requirements and provide a certificate of insurance.
> 2) Commercial General Liability Policy per occurrence - $1,000,000. Coverage to include bodily injury and property damage combined single limit.
> 3) Business Automobile Policy to include but not limited to liability coverage on any owned, non-owned, or hired vehicle used by Data Communications Provider's authorized contractor personnel in the performance of this Master Agreement. The business automobile policy shall have the following limits of liability: Per Occurrence - $1,000,000, Annual Aggregate - $3,000,000, Annual Aggregate applying to products and services - $3,000,000. Coverage must include premises and operations, bodily injury and property damage, personal and advertising injury; blanket contractual, products and services, owner named as an additional insured. The State of Utah must be listed as an additional insured.

Within 10 days of contract award, the Contracted Supplier and/or Authorized Contractor must submit proof of certificate of insurance that meets the above requirements or the Participating States requirements.

Cisco Response:

Read and understood. Please see Cisco's responses to Section 15 of the WSCA-NASPO Standard Terms and Conditions and to Sections 36 and 37 of the State of Utah Additional Terms and Conditions.

3.1.4 Delivery

(M) The prices offered shall be the delivered price to any WSCA-NASPO purchasing entity. All deliveries shall be F.O.B. destination with all transportation and handling charges paid by the contractor. Responsibility and liability for loss or damage shall remain the Contractor until final inspection and acceptance *(within 30 days after delivery for external damage and 30 days for any concealed damage)* when responsibility shall pass to the Buyer except as to latent defects, fraud and Contractor's warranty obligations. The minimum shipment amount will be found in the special terms and conditions. Any order for less than the specified amount is to be shipped with the freight prepaid and added as a separate item on the invoice. Any portion of an order to be shipped without transportation charges that is back ordered shall be shipped without charge.

Cisco Response:

Read and understood. Please see Cisco's response to Section 8 of the WSCA-NASPO Standard Terms and Conditions on "Delivery."

3.1.5 Service Offering Documentation

(M) Upon request, user and/or technical documentation should be supplied for all procured products and services. Manuals may be available via the Contracted Supplier's website. The manual shall contain user and technical instructions appropriate to the service.

Cisco Response:

Read and understood. The extensive information available on the Cisco Technical Support and Documentation web pages preempts most calls to the Cisco TAC and allows customers to resolve seventy nine percent (79%) of their network problems without ever having to pick up the phone. Cisco.com automates a wide variety of tools and processes, including a set of Internet commerce tools that allows customers to buy Cisco products and services online and check the availability and status of spare parts. Cisco.com also automates the troubleshooting of many common support issues.

3.1.6 Data Communications Provider Contract Administrator and Usage Report Administrator

(M) The Contracted Supplier shall provide a Contract Administrator to manage compliance with the scope and terms and conditions for this contract. The following Information, at a minimum, regarding the Contract Administrator shall be provided:

a. Administrator's number of years experience in the Data Communications Services business.

Cisco Response:

Contract Administrator

Mimi Nguyen
Sr. Manager, U.S. Public Sector Contracts Management Office
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134
Office: 408.527.2627l **Fax:** 408.608.1802 I **Email:** mimnguye@cisco.com

Experience: 6+ years in the Data Communications Services Business. 19+ years in High Tech Contracts Negotiations and Management.

b. Confirmation that the Data Communications Provider Contract Administrator has authority to enforce the scope of work and terms and conditions of the resulting contract.

Cisco Response:

Confirmation: Ms. Nguyen has the authority to enforce the scope of work and terms and conditions of the resulting contract.

The Contracted Supplier shall also provide a Usage Report Administrator responsible for the quarterly sales reporting described in Section 1.15 Usage Reporting Requirement.

Cisco Response:

Usage Report Administrator

Angelene Feril*
Gov/Ed Manager, U.S. Public Sector Contracts Management Office
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134
Office: 408.424.0712 I **Fax:** 408.608.1729 I **Email:** aferil@cisco.com

Experience: 12+ years in the Data Communications Services Business. 5+ years in High Tech Contracts Negotiations and Management.

*Ms. Feril also has delegated authority to enforce the scope of work and terms and conditions of the resulting contract in Ms. Nguyen's absence, as necessary.

3.1.7 eMarket Center Cooperation

(M) To be eligible for contract award, the Contractor must agree to cooperate with WSCA-NASPO and SciQuest (and any authorized agent or successor entity to SciQuest) with uploading a hosted catalog or integrating a punchout site. The contract requirements are in section 7.

Cisco Response:

Read and understood. Please see Cisco's response to Section 7.

Section 4: Data Communications Provider Qualifications

4.1 General Information:

Provide any pertinent general information about the depth and breadth of the Offeror's product and service offerings and their overall use and acceptance in the Data Communications marketplace.

Cisco Response:

Cisco Products and Services

Cisco offers a wide range of products and services designed for enterprises and small businesses across a variety of industries.

Borderless Networks

Cisco Borderless Networks connects people, information, and devices – securely, reliably, and seamlessly. The Cisco Borderless Networks product suite includes:

- Switches: Expect more from your network, and save more on operations through innovations such as Cisco EnergyWise
- Routers: Deliver a superior customer experience, increased architectural scalability, and investment protection

- Security: Reduce costs and complexity with an architectural and systems approach to security
- Wireless: Highly reliable, mission-critical Cisco 802.11n networks that accelerate innovation for small to large businesses
- Management: Simplify network management, reduce errors, and speed troubleshooting while reducing operations costs
- WAN Optimization: Accelerate applications over the WAN, consolidate branch infrastructure, and empower cloud computing.

Borderless Network Solutions

Cisco Borderless Network Solutions help accelerate business growth, control energy costs, scale video, and deliver highly secure wired and wireless access.

- The Cisco Borderless Network Architecture is built on an infrastructure of scalable and resilient hardware and software (**Figure 4**). Components of the architecture come together to build network systems that span your organization from network access to the cloud. Intelligent network, endpoint, and user services provide the flexibility, speed, and scale to support new devices, applications, and deployment models.

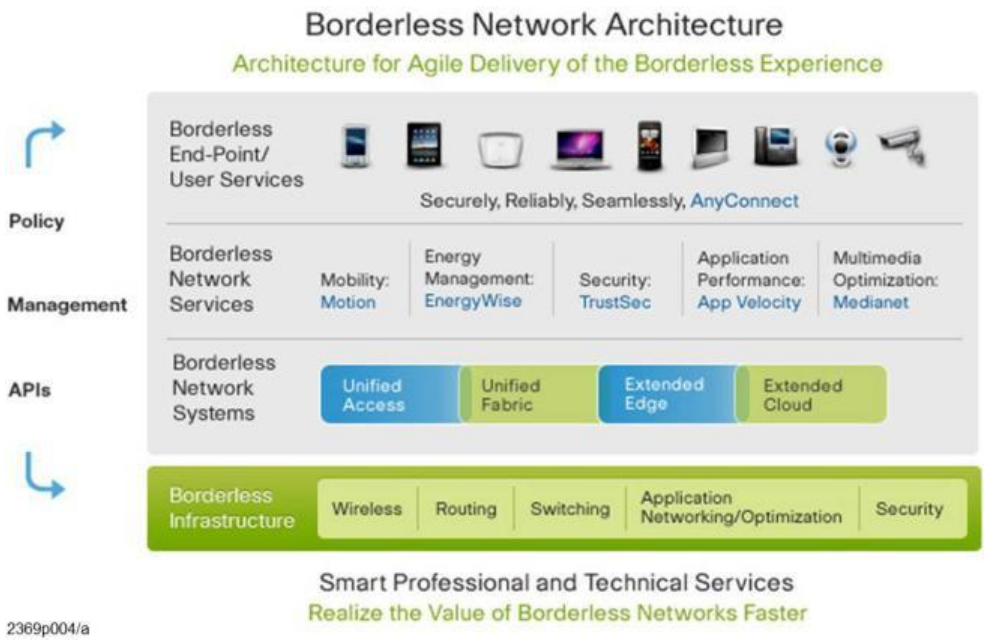

Figure 4. Cisco Borderless Network Architecture

Collaboration

Cisco Collaboration enables your people to communicate more naturally, anywhere, anytime. The Cisco Collaboration product suite includes:

- Customer Care: Customer care creates the foundation for positive customer service, a primary factor in building a stronger business
- Conferencing: Voice, video, and web conferencing lets you keep the work moving without leaving the office
- Enterprise Social Software: Connect people with relevant resources and expertise
- IP Communications: View, optimize, and manage your entire communications system from one screen

- Messaging: See who is available, choose the best channel, and communicate
- Mobile Applications: Take your desktop with you and meet anywhere you can use your phone
- TelePresence: Cisco TelePresence powers a new way of working where everyone, everywhere can be more productive through face-to-face, immersive collaboration.

Cisco Collaboration Solutions

Cisco Collaboration Solutions provide a "new way to work" by addressing the business requirements of a post-PC era with a workplace that is more mobile, social, visual, and virtual.

The Cisco Collaboration Architecture gives your employees, customers, and partners ways to instantly contact you, interact, and conduct business – through the communications channels they prefer, and achieve these business objectives (**Figure 5**). The elements of the Cisco Collaboration Architecture establish a collaboration core that powers compelling experiences both within and among organizations. Working together in a modular fashion, these capabilities allow you to develop an investment plan that helps ensure interoperability with your existing assets.

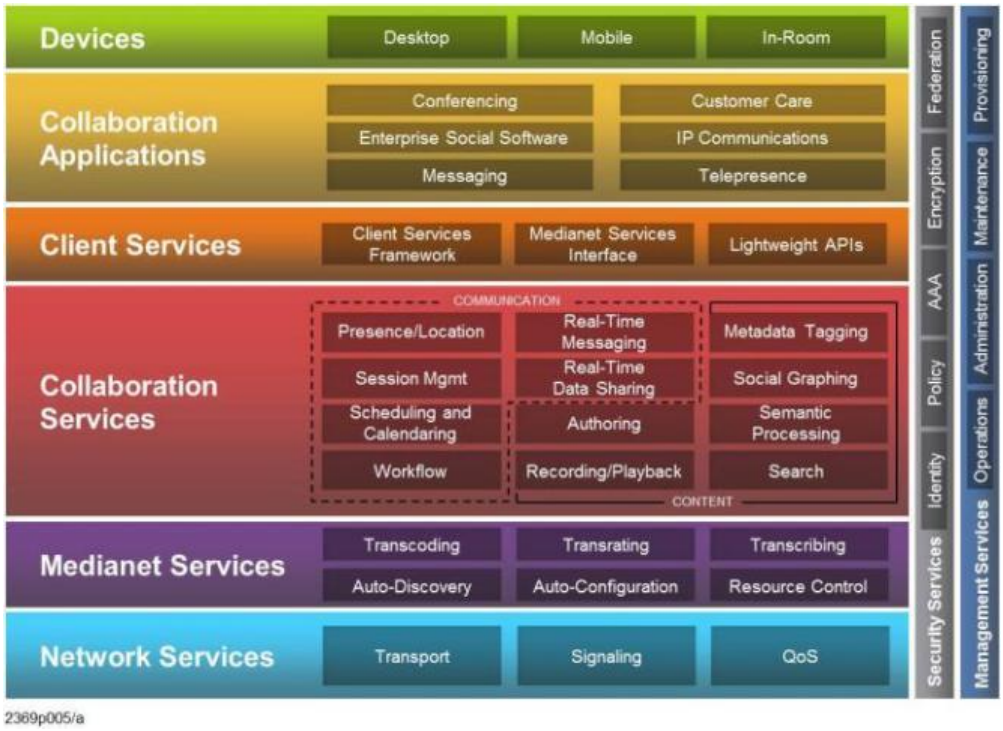

Figure 5. Cisco Collaboration Architecture

Data Center and Virtualization Products

Cisco Data Center and Virtualization helps decrease costs, enhance scalability, and improve data center performance with unified computing. The Cisco Data Center and Virtualization product suite includes:

- Data Center Switching: Increase business agility, simplify operations, and protect your investment with the architectural flexibility provided by data center switching
- Data Center Management and Automation: Increase efficiency with IT automation products that save time, provide clear visibility, and strengthen control over operations
- Storage Networking Solutions: Deploy Cisco Unified Fabric solutions with unified management to simplify operations, enhance agility, and improve flexibility

- Application Networking Solutions: Protect critical applications, infrastructure, and data while increasing application availability and reducing costs
- Data Center Security: Secure your critical applications, infrastructure, and data while ensuring data privacy and regulatory compliance
- Unified Computing System: Scale service delivery and simplify requirements for data center setup, management, power, cooling, and cabling.

Services Portfolio

Advanced Services (e.g., SMARTnet, etc.): Our services drive technology integration while helping lower operational costs, increase network availability, and optimize performance.

- **Technical Services/Maintenance Services**: We help ensure Cisco products and your network operate efficiently and benefit from up-to-date system and application software.
- **Remote Management Services**: We take the lead in co-managing your Cisco Advanced Technology network around the clock. Enjoy lower TCO and focus on your core business without giving up control of your network.

Data Center Solutions

Cisco Data Center Solutions helps reduce costs, deliver superior scalability, are easy to manage, and simplify operations.

The Cisco Unified Data Center is based on three pillars of Cisco innovation: Unified Fabric, Unified Computing, and Unified Management (**Figure 6**). It provides a superior foundation for cloud computing by unifying computing, networking, storage, and management in a common platform designed to automate deployment and management across physical and virtual resources for superior delivery of IT-as-a-Service (ITaaS).

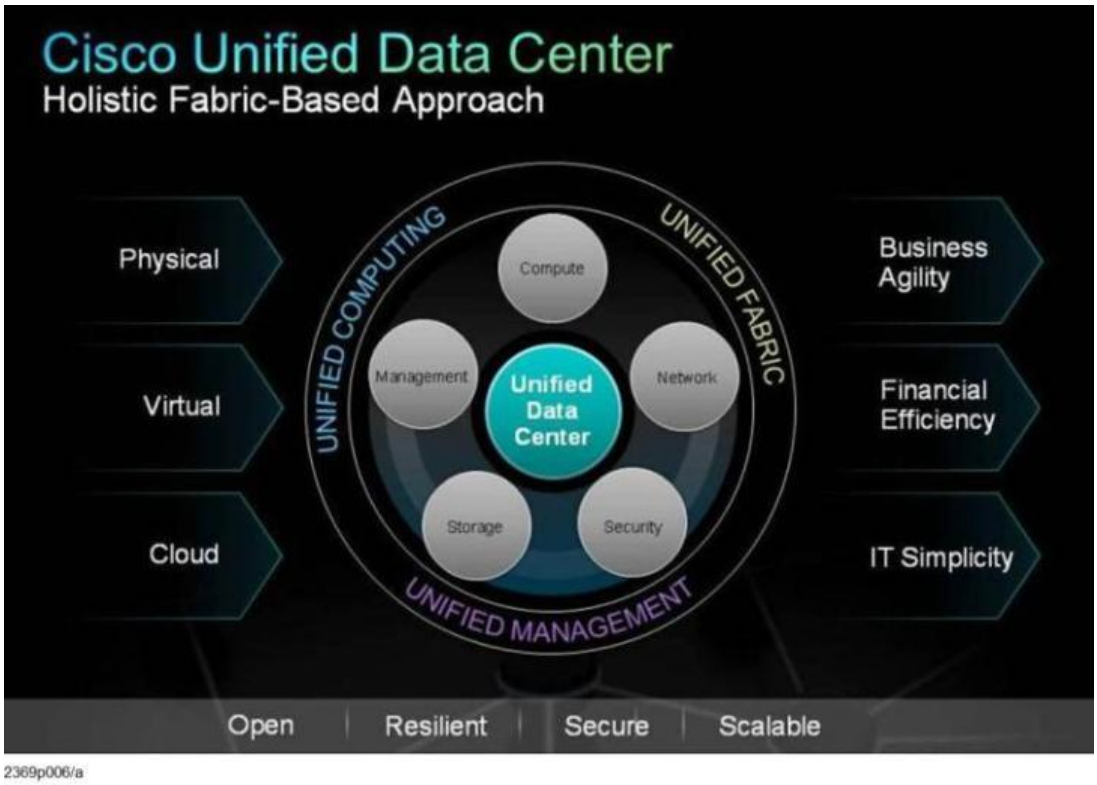

Figure 6. Cisco Unified Data Center

4.2 Warranty

Specify the Offeror's standard warranty offerings for the products and services proposed in the response to this RFP.

Cisco Response:

All Cisco hardware and software products are covered for a minimum of 90 days. Some products have a longer or more appropriate coverage. All Cisco warranties apply to the Customer or Original Owner (the individual who purchased the product for their own use) also referred to as the End User.

Note: All Cisco warranties are subject to and provided only on the terms and conditions set out in the Cisco Limited Warranty, Disclaimer of Warranty, and End User License Agreement.

Following please find our Standard Limited Warranty. For a complete list of Cisco product warranties and customer entitlements under these warranties, please see:
http://www.cisco.com/en/us/products/prod_warranties_listing.html

Cisco Standard Limited Warranty Terms for Products:

Hardware: Cisco Systems, Inc., or the Cisco Systems, Inc. subsidiary selling the Product ("Cisco") warrants that commencing from the date of shipment to Customer (and in case of resale by a Cisco reseller, commencing not more than ninety (90) days after original shipment by Cisco), and continuing for a period of the longer of (a) ninety (90) days or (b) the period set forth in the warranty card accompanying the Product (if any), the Hardware will be free from defects in material and workmanship under normal use. The date of shipment of a Product by Cisco is set forth on the packaging material in which the Product is shipped. This limited warranty extends only to the original user of the Product. Customer's sole and exclusive remedy and the entire liability of Cisco and its suppliers under this limited warranty will be, at Cisco's or its service center's option, shipment of a replacement within the warranty period and according to the replacement process described in the warranty card (if any), or if no warranty card, as described on the Cisco Product Warranties Web page www.cisco.com/go/warranty or a refund of the purchase price if the Hardware is returned to the party supplying it to Customer, freight and insurance prepaid. Cisco replacement parts used in Hardware replacement may be new or equivalent to new. Cisco's obligations hereunder are conditioned upon the return of affected Hardware in accordance with Cisco's or its service center's then-current Return Material Authorization (RMA) procedures.

Software: The limited warranty in the WSCA-NASPO Master Agreement Terms and Conditions and the End User License Agreement sets forth Cisco's warranty obligations with respect to the Software. The End User License Agreement may be located at the following URL: http://www.cisco.com/go/eula

Product warranty terms and other information applicable to the Product may be located at the following URL: http://www.cisco.com/go/warranty

Restrictions: The above Hardware warranty and limited warranty in the End User License Agreement ("Software Warranty") do not apply if the Software, Hardware Product, or any other equipment upon which the Software is authorized by Cisco or its suppliers or licensors to be used (a) has been altered, except by Cisco or its authorized representative, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Cisco, (c) has been subjected to abnormal physical or electrical stress, abnormal environmental conditions, misuse, negligence, or accident; or (d) is licensed for beta, evaluation, testing, or demonstration purposes. The Software warranty also does not apply to (e) any temporary Software modules; (f) any Software not posted on Cisco's Software Center (on Cisco.com URL where Cisco makes the Software publicly available to licensed customers); (g) any Software that Cisco expressly provides on an "AS IS" basis on Cisco's Software Center; or (h) any Software for which Cisco does not receive a license fee.

Disclaimer of Warranty:

Except as specified in this warranty section, all express or implied conditions, representations, and warranties including, without limitation, any implied warranty or condition of merchantability, fitness for a particular purpose, non-infringement, satisfactory quality, non-interference, accuracy of informational

content, or arising from a course of dealing, law, usage, or trade practice, are hereby excluded to the extent allowed by applicable law and are expressly disclaimed by Disco, its suppliers and licensors. to the extent an implied warranty cannot be excluded, such warranty is limited in duration to the express warranty period. Because some states or jurisdictions do not allow limitations on how long an implied warranty lasts, the above limitation may not apply, These warranties give customer specific legal rights, and customer may also have other rights which vary from jurisdiction to jurisdiction.

This disclaimer and exclusion shall apply even if the express warranty set forth above fails of its essential purpose.

4.3 Website

Award contractors are required to establish and maintain a website applicable to the WSCA/NASPO contract which will allow Participating States to see applicable contract price list, discounts on said price list, approved resellers or partners for their state and any additional information that may be required to assist the participating states in obtaining information concerning the contract award. The State of Utah representing WSCA/NASPO reserves the right to require the award contractor to add additional items to assist in this process. Specify Websites used by the Offeror to facilitate customer ordering under awarded contracts.

This is a mandatory requirement.

Cisco Response:

Read and understood. Cisco intends to establish and maintain a WSCA-NASPO contract website at www.Cisco.com similar to what Cisco currently has today. Under the existing Cisco WSCA Data Communications AR-233 contract, Cisco currently maintains a WSCA website at the following URL: http://www.cisco.com/web/strategy/government/wsca/index.html. The website will contain dedicated pages for each individual Participating Entity that executed a Participating Addendum. Each Participating Entity's webpage will have the applicable/approved price lists and discount information, contract document copies; ordering instructions for customers; related link to the WSCA-NASPO website; list of Authorized Resellers for that specific Participating Entity including their general company information, contact people information, and any additional, incremental discounts as applicable per each Authorized Reseller.

4.4 Customer Service

Specify the Offeror's standard customer service policies and detail the escalation process used to handle customer-generated issues.

Cisco Response:

For customers with current Cisco service contracts, Cisco provides technical support services 24 hours per day, 7 days per week, on the web and over the phone.

Technical Related Issues. When a customer purchases SMARTnet and/or any of Cisco's other Technical/Maintenance Services, the customer will have access to the Cisco Technical Assistance Center (TAC). TAC has a formal process in place for handling and responding to customer case-escalation requests. To help ensure all service requests are reported in a standard format, TAC has established the following service request severity definitions, as shown in **Table 1**.

Table 1. Service Request Severity Definitions

Severity Level	*Definition*
Severity 1 (S1)	Your network is "down" or there is a critical impact to your business operations. You and Cisco will commit considerable resources around the clock to resolve the situation.
Severity 2 (S2)	Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected. You and Cisco will commit considerable resources during normal business hours to resolve the situation.
Severity 3 (S3)	Operational performance of your network is impaired, while most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.
Severity 4 (S4)	You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

If you feel that progress on your service request or the quality of Cisco Services is not satisfactory, Cisco encourages you to escalate the service request. You can do this by contacting the TAC and asking for the TAC duty manager. Online resources and phone numbers for contacting the appropriate Cisco TAC are available at: http://www.cisco.com/en/us/support/tsd_cisco_worldwide_contacts.html

As part of ISO standards for escalation process workflow, email alerts are generated by the TAC trouble ticketing system, notifying the individuals listed in **Table 2** if no activity (update or status change) is recorded against a service request for the following periods. Severity 1 alert times are measured in calendar hours — 24 hours per day, 7 days per week. Severity 2 alert times corresponds with standard business hours.

Table 2. Automatic Email Alert Escalations for Cisco TAC Service Requests

	Severity 1 Network Down	*Severity 2 Severe Impact*
1 Hour	TAC Manager	
4 Hours	TAC Director	TAC Manager
24 Hours	VP Customer Advocacy	TAC Director
48 Hours	President	VP Customer Advocacy
96 Hours		President

Continuous improvement in service quality is driven and measured by the use of customer satisfaction surveys. Cisco uses both relationship and transactional surveys to identify strengths and opportunities for improvement. Organizational, management, and individual goals and objectives are established based on the results of these surveys. Improvement plans are developed based on the key messages from the surveys and progress is tracked and reported at monthly and quarterly reviews.

4.5 Firm

a. Provide a brief history of your firm including the following:

1. Number of years providing Data Communications Services being offered in response to this RFP.

Cisco Strategy:

Solve our customers' most important business challenges by delivering intelligent networks and technology architectures built on integrated products, services, and software platforms.

Cisco Response:

At Cisco, our customers are our top priority. We value our partnerships with our Public Sector customers to find solutions to challenging problems that will ultimately improve the lives of citizens.

The concept of solutions being driven to address specific customer challenges has been with Cisco since its inception. Since then, Cisco has shaped the future of the Internet by creating unprecedented value and opportunity for our customers, employees, investors, and ecosystem partners and has become the worldwide leader in networking - transforming how people connect, communicate, and collaborate. Cisco has been providing Data Communications solutions since 1984, for a total of 29 years.

2. Number of separate services provided in each of the area categories described in this RFP.

Cisco Response:

Cisco and our partners offer a comprehensive family of IT services. Regardless of the technology that a customer is deploying, Cisco's holistic services approach provides customers with the necessary tools to analyze and implement technology during every portion of their IT lifecycle. From the planning phase, to building phase, to the managing phase, customers can rely on Cisco services.

Our service model is designed to allow customers to leverage Cisco services for their specific technology no matter where they are on the IT lifecycle. Whether a customer needs help with completing an assessment to decide on a new IT investment, to low level or high level network design, to optimization services to harness the most out of an existing IT infrastructure, Cisco's service offerings can be paired to match customer needs.

A detailed description of Cisco's services portfolio is provided under sections 5.3.1.1 and 5.3.1.2.

b. Describe specifically what makes your firm a stable long term partner for WSCA-NASPO.

Cisco Response:

Based on Cisco's financial strength, robust portfolio of offerings and talented workforce, Cisco can confidently be relied upon as a stable, long-term partner for WSCA-NASPO.

- **Experience** — 29 years in the Data Communications/Networking Business.
- **Creditworthiness** — Dun & Bradstreet Composite Rating of 5A2.
- **Strong Performance** — Financials for 2012 and 2013 included net sales of over $46.1 billion and $48.6 billion respectively.
- **Cash on Hand** — During periods of uncertainty, our strong balance sheet continues to be a competitive advantage. Total assets were $92.6 billion at the end of fiscal 2013, including $47.7 billion in cash, cash equivalents, and investments held globally.

- **Broadest Portfolio of Products** — Cisco has the broadest portfolio of networking/data communications products as is evidenced by our market leadership (#1, #2) across almost all of our technology sectors:
  - #1 in Routing: Edge, Core, Access
  - #1 in TelePresence
  - #1 in Wireless LAN
  - #1 in Switching: Fixed, Modular
  - #1 in Voice
  - #1 in Web Conferencing
  - #1 in Security
  - #2 in Storage Area Networks.
- **Acquisitions** — Cisco's growth strategy is based on identifying and driving market transitions. Corporate development focuses on acquisitions that help Cisco capture these market transitions. Cisco has acquired over 150 companies during its history.
- **Partner/Reseller Community** — Our Cisco-certified resellers combine their deep industry knowledge and Cisco's 29 years of networking experience and tools to optimize our customers' network infrastructure. In the U.S. alone, Cisco has 15,439 partner resellers currently. Outside the U.S., Cisco has 51,711 resellers.
- **Dedicated Public Sector Employees** — As of Q2 FY 2013, Cisco had 73,460 employees. 1076 of these are dedicated to U.S. Public Sector.
- **World-Class Technical Support Services 24/7** — Cisco Technical Support Services are the gateway to the Cisco Technical Assistance Center (TAC), providing 24-hour 24/7 troubleshooting and technical support services for Cisco customers globally, both online and over the phone. This organization enhances administrator productivity and self-sufficiency by providing access to Cisco technical engineering staff and comprehensive documentation, tools, and labs.
- **Spare Parts Distribution Centers across the Globe** — Over 900 spare parts depots with over 170,000 parts delivered every quarter.

In addition, Cisco has successfully demonstrated it is a trusted and reliable partner through the current Cisco WSCA Data Communications AR-233 contract. Cisco is tremendously proud of its existing agreement and the impacts that we have made in helping our WSCA-NASPO government customers serve, protect, and improve the lives of its citizens and communities. For the past 5 years, Cisco has provided its offerings up to 19 Participating States and all the authorized users (local governments, schools, etc.) under those states. From Q1CY2008 – Q2CY2013, Cisco has sold over $679 million of its products and services under our current WSCA contract in partnership with 175 Authorized Resellers across the United States. And, to date, we are pleased to have remitted $3.3 million in administrative fees to WSCA and $2.9 million total to those Participating States who also have their own administrative fees.

To ensure that each of the current Participating States and its authorized purchasers are supported appropriately, we rely on our Cisco certified resellers across the U.S. to provide "feet on the street" from geographic coverage to the necessary expertise in Cisco technologies. Under each current Participating Addendum, we carefully vet and select the authorized resellers ("Authorized Resellers") after consultation with the Participating State. We understand the importance of promoting economic development and supplier diversity in each Participating State as well as simply taking care of those towns, cities, and K-12 schools in remote areas. Our reseller selection process is both thorough and comprehensive as we take into account the needs and requirements of each Participating State, the various buying entities, and the constituents that they serve. The end result is to provide the authorized purchasers of each Participating Addendum with Cisco certified resellers that they can rely on for their data communication needs.

c. Describe specifically what information the Data Communications Provider contract administrator would provide at annual meetings with an entity that has executed a participating addendum.

Cisco Response:

Cisco's WSCA-NASPO Contract Administrator would be pleased to provide the following information at annual meetings with a Participating Entity that has executed a Participating Addendum:

- Total Sales for the Year under that Participating Addendum (Total, Products Sales, Services Sales)
- Total sales by type of Purchasing Entity vertical (State, Local, K-12, Higher Education) under that Participating Addendum
- Total Administrative Fees Paid to Participating Entity (if applicable for that Participating Addendum)
- Highlights of major projects and accomplishments under the Participating Addendum (i.e., customer success stories, marketing activities, operational efficiency, etc.)
- Status Update on the Authorized Resellers under that Participating Addendum
  - Changes (adds, removals)
  - Specializations; expertise and coverage areas
  - Sales total by each Authorized Reseller
  - Reseller Performance Management Activities (i.e., training, reviews/evaluations, etc.)
- What's New at Cisco
  - New offerings and technologies
  - Acquisitions and integration timelines
- Contracts Management Process Improvement Initiatives for the following year
- Marketing plans for the following year.

d. Describe how you plan to implement the contract including having a single point of contact to perform and manage all aspects of this contract.

Cisco Response:

As with the current WSCA Data Communications AR-233 contract that Cisco holds today, Cisco's U.S. Public Sector Contracts Management Office ("Cisco's CMO") will continue to manage and administer the new contract with proven commitment to customer satisfaction. Ms. Mimi Nguyen, Sr. Manager, will continue to be the single point of contact and be responsible for general oversight of the new WSCA-NASPO Master Agreement and program. Ms. Angelene Feril, Gov/Ed Manager, will be leading the efforts to operationalize the new WSCA-NASPO Master Agreement and each Participating Addendum that gets executed, including the onboarding of the selected resellers for each Participating Addendum and overseeing the submission of the quarterly usage reports and administrative fees.

Cisco has already prepared a roadmap of all the major tasks that need to be timely completed in order to successfully implement the new WSCA-NASPO contract and ensure a smooth transition from the current one. **Table 3** below describes our high-level implementation roadmap. Detailed project plans will be created for each major task. With over 5 years of experience in operationalizing the current WSCA Data Communications AR-233 contract and 19 Participating Addendums, Cisco is prepared with the appropriate resources, systems, and tools to efficiently roll-out the new WSCA-NASPO contract and Participating Addendums, and effectively administer the contract.

Table 3. High-Level Implementation Roadmap

#	Major Tasks	Activities	Date	Participants
	New Data Communications Agreement Released, Bid Response and Review by WSCA-NASPO	■ WSCA Utah Releases RFP ■ Cisco Responds	Jul 1 – Aug 30, 2013	■ WSCA Utah ■ Cisco
	Contract Award and Negotiations with OEMs	■ WSCA Utah Awards Contracts to OEMs ■ WSCA Utah Negotiates with Awarded OEMs	TBD	■ WSCA Utah and Legal ■ Cisco CMO and Legal
	Cisco/WSCA-NASPO Master Agreement Executed and Cisco Negotiates New Participating Addendums ("PAs") with Participating Entities ("PEs")	■ WSCA Utah and Cisco Execute New Master Agreement ■ Cisco begins negotiating new PAs with PEs ■ To expedite PA negotiations process, Cisco will prepare a "Cheat Sheet" that compares the differences between the "old/existing" Master Agreement vs. "new" Master Agreement ■ Provide WSCA Utah the "Cheat Sheet" for review and approval before releasing to Participating Entities	TBD	■ WSCA Utah/PEs ■ Cisco
	Vetting and Selecting Resellers for Each Participating Addendum/Participating Entity	■ Consult with each Participating Entity to identify specific needs and requirements relating to the new resellers ■ Canvas interested resellers and send out application ■ Review responses, identify proposed list of resellers, and submit for approval by Participating Entity for each PA	TBD	■ Cisco ■ PEs ■ Interested Resellers
	Reseller Onboarding	■ Due Diligence Checks on selected resellers (Legal, Financial) ■ Resellers execute subcontracts, Discount Letters, and other required paperwork by Participating Entity ■ June 1, 2014 – New Contract is LIVE	TBD	■ Cisco ■ WSCA Utah/PEs ■ Interested Resellers

#	Major Tasks	Activities	Date	Participants
	Update Contract Websites at Cisco.com and Reporting Tool	■ WSCA-NASPO updates WSCA's Own Website with new Master Agreement ■ Cisco updates WSCA-NASPO Contract Webpages at Cisco.com and Cisco's Reporting Tool; Update each Participating State's PA, reseller list, etc.	TBD	■ WSCA Utah ■ Cisco
	Training	■ Train ALL approved/authorized resellers in Participating Entities ■ Train Cisco Sales and Channels Teams ■ Train Participating Entities' Administrators (as necessary – i.e., new folks) to access quarterly reports through Cisco's reporting tool	TBD	■ Cisco (Trainer) ■ Authorized Resellers ■ PEs
	Marketing Campaign	■ Prepare and submit proposed materials for approval	TBD	■ Cisco ■ WSCA Utah/PEs
	Ongoing Contracts Management and Compliance	■ Quarterly Sales Reporting and Administrative Fees Remittance ■ Reseller Performance Reviews ■ Customer Satisfaction	Term of New Contract	■ Cisco ■ Authorized Resellers

e. Describe in detail your firm's escalation management plan including contact information.

Cisco Response:

Contracts Related Issues: For contracts management and administrative related issues or concerns, below is the following key contact information:

Mimi Nguyen
Sr. Manager, U.S. Public Sector Contracts Management Office
Cisco Systems, Inc.
Office: 408.527.2627 I **Fax:** 408.608.1802 I **Email:** mimnguye@cisco.com

Angelene Feril
Gov/Ed Manager, U.S. Public Sector Contracts Management Office
Cisco Systems, Inc.
Office: 408.424.0712 I **Fax:** 408.608.1729 I **Email:** aferil@cisco.com

The following escalation management plan is currently in place today for the purpose of timely addressing any contractual issues and/or concerns raised by our WSCA-NASPO customers:

- **Review and Appropriate Escalation.** Upon notification of an issue or concern by a customer and after performing the necessary review and investigation, Cisco's U.S. Public Sector Contracts Management Office (Cisco's CMO) will lead the effort to properly communicate the matter to the appropriate internal and external stakeholders for action, including senior management of all parties involved as necessary. For example, issues may be escalated to Cisco management in Sales, Channels, Legal, Finance, and/or other impacted Cisco department(s) as required to properly evaluate and address the issue or concern. If the matter is related to one of its Authorized Resellers, Cisco's CMO will also reach out to that Authorized Reseller and its management sales team accordingly.
- **Corrective Actions.** Depending on the nature the issue, the appropriate corrective actions within Cisco's control will be identified and implemented, as Cisco deems necessary or commercially reasonable to execute in order to ensure satisfactory resolution. Cisco's CMO will keep WSCA Utah and/or the Participating State or Entity apprised of its progress. Where the corrective action requires involvement or engagement of external parties, Cisco's CMO will follow-up with such parties appropriately.
- **Feedback and Continuous Process Improvement.** Cisco's CMO welcomes and encourages regular feedback from all of its WSCA-NASPO customers as it continuously strives to maintain operational excellence and customer satisfaction. In addition, Cisco's CMO may also make recommendations for process improvements based on lessons learned and will work with State of Utah and the Participating State or Entity (as applicable) on such initiatives, as appropriate.

Cisco will continue to follow this escalation management plan for the new WSCA-NASPO contract, subject to any continuous process improvements that Cisco may implement.

4.6 Authorized Sub Contractor Relationships

Respondents may propose the use of Servicing Subcontractors or partners however, the Contractor shall remain solely responsible for the performance under the terms and conditions of the Contract if Servicing Subcontractors are utilized. This includes sales report information. The Contractor will be responsible to collect, and report this information from all partners or resellers representing your contract.

a. Briefly describe what your firm requires from potential contractors to become an "Authorized Data Communications Reseller". Provide an Authorized Contractor List.

Cisco Response:

Cisco utilizes a reseller model for sales and order fulfillment and understands that Cisco shall remain solely responsible for the performance of its Authorized Data Communications Resellers ("Authorized Resellers") under the resulting WSCA-NASPO contract. Consistent with the current process under Cisco's existing WSCA Data Communications AR-233 contract, Cisco wishes to defer the selection of the Authorized Resellers until after contract award and upon execution of each Participating Addendum. Based on the RFP's Q&A responses, we interpret that WSCA-NASPO is agreeable to this approach.

Strategic Selection of Authorized Resellers for each Executed Participating Addendum

Cisco understands and is sensitive to the fact that not all of Cisco's resellers have the capacities to sell in every state across the U.S. and to Public Sector customers. Many are small to medium businesses who are focused on selling and supporting certain geographic areas, technology practices, and/or type of Public Sector customer(s) (i.e., state agencies, K-12, etc.). Therefore, to ensure the engagement and participation of diverse resellers, including "local" businesses, our reseller selection process aims to objectively select multiple resellers that can best serve the needs of the Participating State/Entity and the Public Sector customers identified in each Participating Addendum. Cisco will solicit input from the Participating State/Entity who executed a Participating Addendum on its specific needs and/or requirements (i.e., local presence, certain technology expertise, area coverage, etc.).

- Based on the Participating State/Entity's input and Cisco's own business criteria and requirements, Cisco will follow its established process for soliciting and selecting appropriately skilled Authorized Resellers.
- Selected resellers will be expected to (i) "pass" Cisco's legal and financial due diligence checks, and (ii) execute a subcontract with Cisco and adhere to the terms and conditions of the resulting new WSCA-NASPO contract as well as the respective Participating Addendum.

Our application and selection process takes into account, but is not limited to, the following considerations in selecting the resellers that will be authorized to sell to the customer base identified in each Participating Addendum:

- Physical presence within the state (economic development, customer access, etc.)
- Geographic coverage (i.e., north, central, south, remote areas, etc.)
- Reseller's Cisco certification level and technology specializations
- Cisco certified engineering and trained sales resources
- Proven historical Public Sector sales experience and success in the state or geographic locations/territories as identified in the Participating Addendum
- Other value-added services that Cisco and/or the Participating State/Entity may require under that Participating Addendum.

b. Describe in detail how your firm currently measures an authorized contractors' performance.

Cisco Response:

Cisco regularly measures each of Authorized Reseller's performance under the current WSCA Data Communications AR-233 contract per the following criteria:

Compliance and Customer Satisfaction

- Timely submission of the required quarterly sales/usage volume reports. Cisco tracks each Authorized Reseller's submission of its reports via Cisco's reporting web portal tool at https://pos.immixgroup.com/igcisco/.
- Timely submission of the required administrative fees, which are verified and reconciled with Cisco Finance, including proof of payment.
- Timely submission of Participating State/Entity's paperwork or completion or maintenance of certain requirements (i.e., E-Verify documentation, Certificate of Insurance, etc.) as may be required under each Participating Addendum.
- Adherence to the terms and conditions of the Cisco WSCA Data Communications AR-233 contract and each Participating Addendum under which a reseller is authorized to sell.
- Attendance of mandatory trainings provided by Cisco on contracts related topics (i.e., reporting, administrative fees, Ts & Cs, etc.). Cisco provides mandatory training to selected resellers upon execution of new Participating Addendum as part of the reseller's "onboarding" process as well as periodic refresher trainings or updates throughout the term of each Participating Addendum.
- Customer satisfaction (i.e., complaints, feedback, etc.).

Cisco Certifications and Resources

- Maintaining the minimum Cisco certification level as required (i.e., level varies per the needs of each state or geographic location). Cisco verifies that each Authorized Reseller's certification level does not fall below the required minimum level.
- Maintaining the minimum Cisco technology specialization(s) as required (i.e., level varies per the needs of each Participating State/Entity or geographic location). Cisco verifies during the term of the current WSCA Data Communications AR-233 contract each Authorized Reseller's status with respect to the minimum technology specialization(s) required.

- Maintaining the minimum number of engineer and sales resources as required (i.e., number varies per the needs of each Participating State/Entity or geographic location). Cisco verifies during the term of the current WSCA AR-233 contract each Authorized Reseller's resources that were committed during the application process.

Sales Performance

- Authorized Reseller's sales performance under each Participating Addendum
- Participation with Cisco Channels and Sales teams on periodic business reviews
- Marketing/Demand Generation events held by Authorized Reseller to promote the WSCA contract.

c. Describe in detail the process for revoking a designation as a sub contractor from an authorized contractor for issues related to customer service, or other authorized contractor performance related issues.

Cisco Response:

In accordance with and consistent with Cisco's escalation process as set forth in Section 4.5(d) above, Cisco's process for revoking a designation as an Authorized Reseller in connection with customer service-related issues, or other performance-related issues is as follows:

- Cisco will request and obtain all necessary information and details related to the issue from all related parties.
- Cisco will discuss detailed information received with all applicable parties and appropriate departments within Cisco.
- If results substantiate or indicate that the Authorized Reseller was non-compliant in following the terms of its subcontract with Cisco or engaged in acts that were not in the best interest of the customer and/or Cisco, then such Authorized Reseller will be placed on warning status. Cisco will set proper expectations required of the Authorized Reseller to remediate the current issue(s) as well as to prevent any re-occurrence of the issue(s). If special or additional training is required, Cisco will provide as necessary.
- If Authorized Reseller continues with the non-compliant or unacceptable behavior that is not in the best interest of the customer and/or Cisco after being placed on warning, Cisco will then proceed with terminating the subcontracting agreement between Cisco and the Authorized Reseller.

d. Describe in detail how your firm will support and assist an authorized contractor in improving their performance and the corrective action process.

Cisco Response:

Consistent with the current practice under Cisco's existing WSCA Data Communications AR-233 contract, Cisco will continue to support and assist Authorized Resellers in improving their performance and will utilize a corrective action process as necessary:

- **Training.** Upon initial onboarding, Cisco conducts an initial training session of the contract's requirements to all Authorized Resellers. Training will detail critical terms and conditions (i.e., quarterly usage reporting and administrative fee requirements, etc.), clarify common misconceptions, answer frequently asked questions and suggest best practices. Subsequent training sessions are conducted throughout the term of the contract to refresh its subcontractors/resellers as necessary.
- **Business Reviews**. Cisco Partner Account Managers typically conduct periodic business reviews throughout the year to check in with Authorized Resellers and their performance to date on the contract. This provides the Authorized Resellers with the opportunity to gain Cisco's assistance and insight on any issues as well as gain guidance on how to improve their

performance prior to the formal performance reviews. In addition, the Authorized Resellers are encouraged to schedule meetings as needed with their Cisco Sales Account Manager and assigned Partner Account Manager to review their performance and/obtain assistance on how to improve their Cisco practice.

- **Formal Performance Reviews**. Cisco conducts formal performance reviews with its Authorized Resellers, which include verifying compliance with the requirements of the WSCA Data Communications AR-233 contract, Participating Addendums, and Cisco's subcontracting agreement. Authorized Resellers who are found deficient in any of the requirements are given an opportunity to remediate their issues within a specified time period in accordance with an agreed-upon "Get Well Plan". The Get Well Plan generally includes a business plan as well as reasonably attainable goals to remediate each Authorized Resellers identified deficiencies (including compliance-related issues).

e. Describe in detail the process that your firm uses to track and respond to issues and concerns from both your authorized contractors and from participating entities.

Cisco Response:

Customers, subcontractors/resellers, and participating entities contract administrators have multiple parties to communicate issues to in reference to the WSCA/NASPO contract using the following avenues (as applicable depending on the party):

- Cisco Account Managers (assigned to the customer/area)
- Cisco Partner Account Manager (assigned to each reseller)
- Cisco Regional Managers (assigned to the area)
- Cisco System Engineers (assigned to the area)
- CMO Senior Manager (Ms. Mimi Nguyen)
- CMO Gov/Ed Manager (Ms. Angelene Feril)
- CMO Contract Compliance and Administrative Analysts
- ImmixGroup, Reporting Tool Vendor's help desk (via email or phone)
- Authorized Resellers
- CMO help mailer: wsca-help@external.cisco.com
- Participating State Contract Administrator
- WSCA/NASPO Contract Administrator (Utah).

In any event, Cisco's escalation process as set forth in response to 4.5(d) above would be applicable here as well.

f. Describe in detail how your firm will track, report and verify sales from your designated Data Communication partners and authorized contractors.

Cisco Response:

Cisco currently has a comprehensive sales volume report template, which all Authorized Resellers are required to populate with sales volume data and upload to our reporting tool web portal, which has been used to report the current WSCA Data Communications AR-233 contract sales since 2010:

- Web reporting tool is available 24/7 at https://pos.immixgroup.com/igcisco/.
- Automatically tracks all quarterly sales/usage reports submitted.
- Once a report is submitted, Cisco reviews the sales data prior to approving the report. As a manufacturer with the potential of having hundreds of resellers under the new resulting WSCA-NASPO contract as well, Cisco needs the extra time to properly review and process all sales reports received by each Authorized Reseller across all Participating Addendums. (This is why

we appreciate the due dates under our existing contract and are requesting the same timeframes under the new resulting WSCA-NASPO contract as set forth in our bid response to Section 1.15.)

- Once all submissions have been reviewed, approved, and finalized/consolidated in the web portal, Cisco notifies the availability of the reports to the WSCA-NASPO Contract Administrator and all designated Contract Administrators under the executed Participating Addendums.
- Multiple options are available for viewing and/or downloading the data from a high level summary to a full detailed dataset for any given timeframe for which data is available.
- If there are any changes in the Contract Administrators under the resulting WSCA-NASPO contract and/or executed Participating Addendums, Cisco will provide training on how to use the web-reporting tool. Please be advised that such activity (training) is already included in our Implementation Plan as set forth in our response under Section 4.5(c).

Section 5: Service Offering Qualifications

5.1 General Information

This section contains mandatory minimum requirements that must be met in order for your proposal to be considered for the evaluation phase of this RFP. All of the items described in this section are non-negotiable. Respondents are required to complete:

Mandatory Requirements (M)

All Respondents must meet the **(M)** requirements listed in this section, and explain how the requirement is met. A 'no' response on the acceptance document or omission of the required explanation will disqualify the service from further evaluation.

5.1.1 General Business Requirements

Each provider must meet the following mandatory general business requirements:

5.1.2 Terms and Conditions

(M) Respondents *must* indicate their acceptance of the State of Utah Standard Terms and Conditions in addition to the WSCA-NASPO Terms and Conditions attached to this RFP as Attachment A and Attachment B. Any exceptions to these terms and conditions must be clearly identified in bid response and during the question and answer period on BidSync. Significant exceptions may constitute grounds for rejecting Respondent proposals.

Cisco Response:

Read and understood. Please see Cisco's responses/exceptions to the WSCA-NASPO Standard Terms and Conditions and the State of Utah Additional Terms and Conditions in Appendix B and C. Cisco and WSCA have operated successfully with the current terms and conditions for over the last 5 years. As such, we recommend in certain sections that we utilize the terms of our existing agreement. These terms have served all parties well, including the Participating States, which is a testament to the robust and comprehensive nature of the existing agreement. This approach will also serve to expedite reaching final agreement on terms and conditions.

5.1.3 Experience

(M) Respondents *must* be able to provide reference service contracts from a minimum of five government or commercial customers for their Data Communications Product and Services offerings. Government references are preferred. References must include environments and complexity that is similar in scope to those described within this RFP. Any proposals from Respondents that cannot meet these requirements will not be considered. The Respondent must provide specific contact information describing their reference service contracts, which may be verified.

Cisco Response:

Read and understood. The following Cisco government customers have agreed to serve as our references:

1. **Mr. Jack Harris**
   Director, Network Strategy
   DTMB Office of the CTO – State of Michigan
2. **Ms. Christy Ridout**
   Deputy Director, Consolidate Technology Services
   State of Washington
3. **Mr. Haggai Hisgilov**
   Executive Director
   University of California
4. **Mr. Paul Cook**, CPT, PMP
   Business Process Consultant, Senior
   Communications & Technology Management
   City of Austin
5. **Mr. Sam Hanvey**, CPPB, APM
   Team Lead
   Information Technology Management Office
   State of South Carolina
6. **Ms. Jan Pytelewski**, GCPA
   Category Manager - IT Procurement, State Purchasing Division
   State of Georgia - Department of Administrative Services

5.1.4 Financial Stability

(M) The Data Communications Product and Services vendor ***must*** provide audited financial statements to the State and should meet a minimum Dun and Bradstreet (D&B) credit rating of 4A2 or better, or a recognized equivalent rating. Please provide the Respondent's D&B Number and the composite credit rating. The State reserves the right to verify this information. If a branch or wholly owned subsidiary is bidding on this RFP, please provide the D&B Number and score for the parent company that will be financially responsible for performance of the agreement. Prime contractors working on behalf of Respondents must submit financial statements that demonstrate financial stability, and adequate working capital, but do not need to meet 4A2 credit rating requirements.

Cisco Response:

Financial information about Cisco, including annual and quarterly reports, may be found at our Investor Relations page by visiting: http://investor.cisco.com. Please visit the following page to view Cisco financial statements for the past 3 years: http://investor.cisco.com/results.cfm.

Please refer to Cisco's Dun & Bradstreet (D&B) report for the applicable year. Per D&B policy, companies must request this report directly from D&B. Our D&B number is 15-380-4570. Cisco's composite D&B rating is 5A2.

5.1.5 Other General Responsibilities

(M) The Respondent *must* provide the personnel, equipment, tools, and expertise to meet the requirements in this RFP.

Cisco Response:

Read and understood.

(M) Computer applications and Web sites *must* be accessible to people with disabilities, and *must* comply with Participating entity accessibility policies and the Americans with Disability Act.

Cisco Response:

Read and understood. As Cisco changes how people work, live, play, and learn, it is essential that we ensure the same for people with disabilities. That is why we strive to make our products, services, Websites, and documentation accessible and usable by people with disabilities, whether by design or through compatible use with assistive technology.

Accessibility is built into the way we work, the products we develop, and the standards and regulations we follow. It is a responsibility every Cisco employee embraces—because helping all people to contribute equally, regardless of ability, is the right thing to do.

Our Commitment to Accessible Products

The Cisco Accessibility Program is a global company-wide effort that stresses the importance of creating accessible products throughout Cisco, with customers, and with our deployment partners. We help ensure that Cisco products conform to accessibility regulations, and we make accessibility a priority consideration at every stage of the Cisco product lifecycle.

The showcase of the program is the Cisco Accessibility Design and Evaluation Lab, located in San Jose, California. At this location, Cisco works with accessibility experts and people with disabilities to design and build products that are usable by all people. We test and validate with a full range of assistive technologies. We demonstrate how our customer's employees with disabilities can use our products. We benefit from immediate, relevant feedback from our most demanding customers—Cisco employees with disabilities.

The Cisco Accessibility Program maintains detailed, current knowledge of global accessibility and usability laws, regulations, and standards. For example, Cisco tests products against U.S. standards that include Section 508 of the Rehabilitation Act, Section 255 of the Telecommunications Act, and the Americans with Disabilities Act. Internationally, Cisco adheres to guidelines such as those published by the World Wide Web Consortium (W3C). Cisco also contributes to accessibility standards and guidelines created by the International Telecommunications Union (ITU), the Internet Engineering Task Force (IETF), and the Telecommunications Industry Association (TIA).

We approach accessibility with a philosophy of openness, willingly sharing our technological innovations with others through wide participation in industry groups. And we work with third-party vendors to enhance our solutions for broader accessibility.

Review our Accessibility brochure to learn more.

- View Brochure (pdf).

(M) Applications and content delivered through Web browsers must be accessible using current released versions of multiple browser platforms (such as Internet Explorer, Firefox, Chrome, and Safari) at minimum.

Cisco Response:

Read and understood.

5.2 Data Communications Services – Requirements

Offerors may respond to any of the sections where they have substantive product offerings that address the scope detailed in each Section from 5.2.1-5.3.0. All Offerors must include a response to section 5.31 services, that addresses products proposed in 5.2.1-5.3.0.

Products may be used by the states in branch offices, main government offices and data centers, and by overall government data communications providers offering carrier class services. Responses should consider this breadth of use and users.

The scope and context of this solicitation **does not include endpoints such as cell/smart phones, other mobile devices or devices designed exclusively for use by individual users.** It is focused on the equipment and software infrastructure required to support provisioning of a variety of network services within a modern digital network. The user context will vary from branch offices through enterprise and statewide data communication network installations. Respondents should offer a range of solutions that are appropriate for installations of varying size and complexity.

Cisco Response:

Cisco is proposing our entire U.S. Global Price Lists (GPLs) as part of this offering. We feel that our broad portfolio of products meets every category in this RFP. Links to descriptive literature have been provided in each category in order to minimize the size of this response.

In addition to new products, Cisco wishes to offer WSCA-NASPO and the Participating Entities the option to also purchase Cisco Certified Refurbished Equipment (subject to inventory availability) with no compromises and with the same Cisco quality, value, performance, and support as if they were new products:

- **Low Risk; Same Warranty as New**. Backed by the same Cisco warranty and support options as new products through Cisco Technical Assistance (TAC).
- **Peace of Mind; Certified Protection**. Fully remanufactured to like-new condition using ISO 9001/14001 certified processes and reconditioned to Cisco specifications. Certified to meet all regulatory and safety compliance requirements such as FCC, CE, and UL.
- **Award-Winning Technical Support Service**. Eligible for the same maintenance and service support (SMARTnet) as new products, which provides direct access to Cisco's TAC, 24 hour/365 day access to www.cisco.com support resources, access to minor and major OS releases, rapid hardware replacement, and options for onsite engineer support.
- **Optimum Performance**. Latest proprietary hardware and software upgrades help ensure maximum in-network performance, reliability, compatibility, and future scalability. Fully licensed and shipped with valid Cisco IOS Software license.
- **Extensive Inventory**. Over 3500+ different new and end-of-sale products; across all technologies on Cisco's price list.
- **Increase Budget Flexibility**. Value priced with no hidden costs—up to 80 percent off list price of equivalent new product. Such competitive pricing and financing will enable WSCA-NASPO Participating Entities to get the most network solutions with their limited technology budgets.
- **Fast Shipping**. In-stock inventory typically ships within 24-48 hours from multiple warehouse locations.
- **Available only through Authorized Resellers**. Only resellers who have been vetted by Cisco Systems to participate under the respective Participating Addendum can sell Cisco Certified Refurbished Equipment. Additional assurance that WSCA-NASPO Participating Entities are buying from verified and approved sources.

More information about Cisco Certified Refurbished Equipment is available at:
http://www.cisco.com/web/ordering/ciscocapital/refurbished/index.html

Cisco's products are generally integrated into solutions or architectures for a majority of technology categories listed in this RFP. Server products and associated software are integral components of many of these networking solutions and architectures. These solutions simply cannot not be implemented, nor meet our customers' basic operational expectations and requirements, without the included server components. Therefore, Cisco is offering server products and software as part of our integrated solutions where required, but not as a separate stand-alone product category. For example, regarding our collaboration portfolio, Cisco Unified Computing System (USC) servers run Cisco Call Manager software, which drives our enterprise telephony platform. Likewise, our Unity products (voice mail) and our E911 solution are driven by UCS servers. Turning to network security, our servers drive the Cisco Identity

Services Engine (ISE) software which is a key component of our security portfolio. Similarly, with regard to network management, our UCS servers host the components that make up the Cisco Prime LAN Management System, including Cisco Prime Network Control System, Cisco Prime Infrastructure, and Cisco Prime Security Manager. It should also be noted that not only do our servers run and drive these solutions they also unify computing, networking, management, virtualization, and storage access into a single integrated architecture that enables end-to-end server visibility, management, and control, thereby enhancing our customers' ability to effectively, efficiently, and economically serve their constituents.

5.2.1 DATA CENTER APPLICATION SERVICES — Application networking solutions and technologies that enable the successful and secure delivery of applications within data centers to local, remote, and branch-office users using technology to accelerate, secure, and increase availability of both application traffic and computing resources.

5.2.1.1 Virtualized Load Balancers — Virtual devices that act like a reverse proxy to distribute network and/or application traffic across multiple servers to improve the concurrent user capacity and overall reliability of applications. Capabilities should include:

- SSL (Secure Sockets Layer) Off-loading
- Caching capabilities
- Layer 4 Load Balancing
- Layer 7 Load Balancing
- Detailed Reporting
- Supports multiple load balancers in the same system for multiple groups
- Supports TLS1.2

Cisco Response:

Cisco is offering our Cisco Virtualization-Aware Networking and Security: Cisco VSG for Nexus 1000V Switches for this category.

Cisco Nexus 1000V Switches provide a comprehensive and extensible architectural platform for virtual machine and cloud networking. The switches are designed to accelerate server virtualization and multitenant cloud deployments in a secure and operationally transparent manner.

Cisco Virtual Security Gateway (VSG) integration with the award-winning Cisco Nexus 1000V Switches is a virtual appliance that provides trusted access to secure virtualized data centers in enterprise and cloud provider environments while meeting the requirements of dynamic policy-driven operations, mobility-transparent enforcement, and scale-out deployment for dense multi-tenancy. Cisco VSG offers IT departments the benefits of workload virtualization with the security of zone-based controls and activity monitoring, enhanced compliance with corporate security policies and industry regulations, and simplified security audits. Cisco VSG helps enable access to trust zones is controlled and monitored through established security policies.

Features and benefits include:

- **Flexible deployment:** Cisco VSG supports both Layer 3 and Layer 2 modes. Additionally, each Cisco VSG protects multiple physical servers.
- **Performance acceleration:** Cisco VSG offloads packet-intensive processing to the switch to optimize performance.
- **High availability:** Deploying Cisco VSG in active-standby mode helps enable high availability.
- **Cloud security:** Cisco VSG extends zone-based firewalling service to virtual machines on VXLAN through updated segmentation features.

Additional details can be found at: http://www.cisco.com/en/us/products/ps13296/index.html

5.2.1.2 WAN Optimization — An appliance utilizing a collection of techniques for increasing data-transfer efficiencies across wide-area networks (WAN). Capabilities should include:

- CIFS (Common Internet File System) acceleration
- Data Compression
- SSL encryption/decryption for acceleration (Optional)
- Layer 4-7 visibility
- Application Specific optimization

Cisco Response:

Cisco Wide Area Application Services (WAAS) currently provides the industry's most scalable, highest-performance WAN optimization solution. Cisco WAAS can improve the end-user experience and reduce bandwidth for applications, including Microsoft Exchange, Citrix XenApp and XenDesktop, SAP, IBM Lotus Notes, NetApp SnapMirror, HTTP and HTTPS, cloud, and file applications.

Cisco WAAS helps enable organizations to implement important business initiatives, including:

- Highly secure, scalable, enterprise-wide Bring-Your-Own-Device (BYOD) solutions
- High-performance Virtual Desktop Infrastructure (VDI) and Cisco Virtual Experience Infrastructure (Cisco VXI)
- Live and on-demand media applications such as webcasting, e-learning, and digital signage
- High-performance, public and private cloud services and Software-as-a-Service (SaaS) applications
- Improved application performance and end-user experience for applications, including web, email, VDI, file, and cloud applications
- Reduced WAN bandwidth requirements and deferral of expensive bandwidth upgrades
- Reduced branch footprint through server and service consolidation
- Data center consolidation, virtualization, and automation.

The features and benefits of the Cisco WAAS solution can be found in **Table 4.**

Table 4. Cisco WAAS Features and Benefits

Benefit	*Feature*
WAN Optimization ■ Eliminate or defer expensive WAN bandwidth upgrades	■ **Transport Flow Optimization (TFO):** TFO improves application packet flow under unfavorable WAN conditions such as packet loss and small initial windows while helping ensure fairness. ■ **Data Redundancy Elimination (DRE):** DRE is an advanced form of network compression that uses a bidirectional database to store previously seen TCP traffic and replace redundant patterns with very small signatures. DRE can provide up to 100:1 compression depending on the data being examined. ■ **Adaptive persistent session-based compression:** This type of compression can provide up to an additional 5:1 compression.
Application Acceleration ■ Improve employee productivity ■ Consolidate branch office servers	■ **Protocol acceleration:** Application-specific latency is reduced through a variety of application-layer techniques such as read-ahead, operation prediction, connection reuse, message multiplexing, pipelining, and parallelization, resulting in LAN-like performance despite deployment over a WAN.

Benefit	Feature
■ Centralize branch office IT resources such as storage and backup tapes, and reduce operating costs	■ **Application optimizers:** Protocol-specific acceleration is available for Microsoft Windows file sharing (Common Internet File System [CIFS]); Microsoft Exchange (Messaging API [MAPI] and MAPI over SSL); encrypted MAPI [eMAPI], HTTP and HTTPS applications such as Oracle, SAP, and Microsoft SharePoint and Outlook Web Access (OWA); Microsoft Windows print services; UNIX Network File System (NFS); and Citrix ICA. These features improve end-user application response times, significantly improving employee productivity. ■ **Content prepositioning:** Centralized policy-based file distribution and prepositioning can be used to push files to edge Cisco WAAS devices, accelerating software patch distribution and file access for all users.
Ease of Initial and Ongoing Deployment	■ **Network transparency:** Cisco WAAS preserves all existing network services. ■ **Client, server, and application transparency:** No modifications to clients, servers, or applications are needed. ■ **Automatic peer discovery:** Cisco WAAS devices automatically discover peers, reducing the number of configuration steps. ■ **Quickstart wizard:** Use of the wizard eliminates many configuration steps. The wizard includes defaults for faster deployment. ■ **Management and monitoring:** Intuitive workflow-based management and real-time monitoring are provided. Diagnostic and troubleshooting tools help reduce Mean Time To Resolution (MTTR).
Flexible Deployment Options for Cloud Computing	For private and virtual private cloud environments: ■ **Agility:** Implement agile virtual machine-based deployments on standard x86 servers, such as Cisco Unified Computing System (Cisco UCS) servers. ■ **Application-specific WAN optimization:** Use Cisco Nexus 1000V Series port profiles and Cisco vPath to create value-added WAN optimization services on a per-application basis in your catalog of cloud services (for example, use Cisco vWAAS only for Microsoft SharePoint or Exchange) for optimized delivery to remote branch office users. ■ **Flexible scale-out Cisco WAAS deployment:** Using policy-based configuration in the Cisco Nexus 1000V Series Switch, you can associate Cisco vWAAS services with application server virtual machines as they are instantiated or moved in response to dynamic application load demand in the cloud. This capability helps enable cloud providers to offer rapid delivery of WAN optimization services with little network configuration or disruption to achieve a cloud consumption and delivery model. ■ **Multitenant:** Cisco vWAAS reduces the hardware footprint needed for multitenant deployments. ■ **DRE on SAN:** Cisco vWAAS offers an option to allow its DRE database to be hosted on the SAN to provide an improved fault-tolerant response and to support virtual machine mobility requirements.

Benefit	Feature
	■ **Validated sizing benchmarks on Cisco UCS servers:** Cisco vWAAS can be hosted on any x86 server that supports the VMware ESX and ESXi 4.0 hypervisor. Sizing benchmarks and performance metrics provided on the Cisco UCS platform result in lower risk for cloud deployments. For public cloud environments: ■ **Accelerated SaaS applications:** Cisco WAAS accelerates SaaS applications, such as Salesforce.com, delivered from the public SaaS cloud. SaaS applications are typically HTTPS-based and can be configured in an easy and scalable manner. In addition, Cisco WAAS Mobile can be used to accelerate access to hosted infrastructure-as-a-service (IaaS) applications delivered from public cloud platforms, such as Amazon.com, to remote mobile users. ■ **Cloud agnostic:** Cisco vWAAS can be deployed in public clouds with the Cisco Nexus 1000V Series to obtain benefits similar to those for private clouds. The Cisco vWAAS solution is public-cloud agnostic.
Delivery of High-Quality Live and On-Demand Video ■ Eliminate need for expensive WAN bandwidth upgrades ■ Avoid complex configuration ■ Centralize branch office video servers	■ **Easy-to-deploy live video with edge-stream splitting:** Automated edge-stream splitting helps ensure that only one video stream is downloaded over the WAN regardless of the number of users in the branch office who are viewing that stream. ■ **Recorded video on demand (VoD):** VoD files can be published using prepositioning on edge Cisco WAAS devices. ■ **Server offload:** Live and on-demand video features offer server offload capabilities that can enable up to a 10 times reduction in the number of data center video servers.
Locally Hosted Branch Office IT Services ■ Reduce branch office device footprint ■ Deploy branch office IT services with flexibility and agility	■ **Network-embedded virtualization:** Third-party services can be hosted on isolated virtual blades. This architecture maintains native performance for WAN optimization while using the same hardware platform for additional hosted services. ■ **Virtual blades:** This feature can be used to deploy many different Microsoft Windows and Linux branch-office services on Cisco WAAS appliances within hours instead of the days or weeks often required for dedicated hardware-based deployments. Certified and supported hosted services include Microsoft Active Directory, Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and print services using Microsoft Windows Server 2003, 2008, or 2008 R2; Cisco Network Analysis Module (NAM); and Cisco Application and Content Network System (ACNS). **Note:** Because Cisco vWAAS is a virtual appliance, it does not support the virtual blades feature available on physical Cisco Wide Area Virtualization Engine (WAVE) appliances.
Simplified Central Management and Monitoring ■ Enhance usability with intuitive workflow-based management tools	■ **Cisco WAAS Central Manager:** This workflow-based tool manages central configuration, provisioning, real-time monitoring, fault management, logging, and customized reporting with the capability to create scheduled reports for up to 2500 Cisco WAAS devices within a Cisco WAAS topology. ■ **Comprehensive statistics:** Comprehensive logs, reports, graphs, and statistics for Cisco Wide Area Application Engine (WAE) device

Benefit	Feature
■ Enhance visibility through real-time monitoring of connections with application performance management	functions help IT administrators optimize system performance and troubleshooting. ■ **Monitoring, reporting, traps, and alerts:** Real-time monitoring of connections, Simple Network Management Protocol (SNMP) Versions 2c and 3, Simple Mail Transport Protocol (SMTP) authentication, and syslog are supported. ■ **Centralized software upgrades:** Administrators can remotely schedule upgrades or version rollbacks. ■ **Application performance management:** NetQoS SuperAgent and Cisco WAAS together uniquely provide accurate reports about end-to-end application response time and WAN bandwidth utilization. ■ **Easy integration with software distribution tools:** Tools include Short Message Service (SMS), LANDesk, Altiris, and BigFix solutions. ■ **XML API:** The XML API can be used to integrate Cisco WAAS Central Manager into customers' network management and monitoring systems.
Scalability and High Availability	■ **Out-of-path deployment:** Cisco WAAS can be deployed using Web Cache Communication Protocol Version 2 (WCCPv2) for high-availability clustering and N+1 load balancing for up to 32 Cisco WAAS devices within a WCCPv2 service group. Policy-based routing (PBR) is also supported as a deployment mechanism. ■ **Physical inline interception:** Cisco WAAS appliances can be deployed transparently using a four-port Network Interface Card (NIC) with fail-to-wire capability in the event of failure, helping to ensure that network connectivity is not lost. The inline option provides high scalability and active-active failover through daisy-chain clustering. ■ **Cisco Application Control Engine (ACE):** Cisco WAAS deployed with Cisco ACE can scale up to 16 million TCP connections and up to 64 Gbps of bandwidth, supporting the largest deployments. ■ **Configuration backup and restore:** In the event of hardware failure, the reprovisioning and restore process can be handled remotely using Cisco WAAS Central Manager. ■ **Redundant WAN link support:** Cisco WAAS supports environments with redundant WAN links, redundant routers, and asymmetric routing to improve high availability and optimization efficiency.
Security	■ **Data-at-rest encryption:** All data on the Cisco WAAS disk is secured with 256-bit Advanced Encryption Standard (AES) encryption and automatic key management. ■ **Data-in-flight security:** Cisco firewalls perform stateful inspection of accelerated traffic. ■ **Acceleration of SSL applications:** Existing enterprise security architecture is preserved when accelerating SSL applications. ■ **Data access security:** All security-related protocol commands are delegated to the file server and the domain controller. No additional domain security or user configuration is necessary. ■ **Management access security:** The Cisco WAAS Central Manager offers authentication, authorization, and accounting (AAA)

Benefit	Feature
	integration with external authentication providers such as Microsoft Active Directory, RADIUS, and TACACS+ and supports role-based access control (RBAC) to help ensure security. ■ **Network security:** Cisco WAAS and Cisco firewalls secure accelerated traffic with stateful firewall inspection and network virus scanning using Cisco IOS Intrusion Prevention System (IPS). No other vendor currently preserves security for accelerated traffic.

Additional information about our WAN optimization solutions can be found at:
http://www.cisco.com/en/us/products/ps5680/products_sub_category_home.html#~featured

5.2.2 NETWORKING SOFTWARE — Software that runs on a server and enables the server to manage data, users, groups, security, applications, and other networking functions. The network operating system is designed to allow shared file and printer access among multiple computers in a network, typically a local area network (LAN), a private network or to other networks. Networking software capabilities should include:

- Restartable Process
- High availability options
- Targeted operating systems, i.e. DC, campus, core, wan, etc.
- Operating System Efficiencies

Cisco Response:

Cisco offers a wide range of solutions that take advantage of the power, platform support, efficiency, and flexibility of Cisco IOS Software.

Consistent Features, Better Usability.

Modular components and feature consistency across our platforms (Cisco IOS, IOS-XR, and NX-OS) are at the core of our new offerings. The ability to share software and maintain consistent features while allowing for reusable code, components and more helps your business, your network, and your teams automate tasks faster and create new services or applications easier than before.

Your Network, Your Way. One Amazing Toolkit.

One Platform Kit (onePK) is Cisco's new easy-to-use development kit that combines robust features of IOS, IOS-XR, and NX-OS across Cisco routers and switches via one abstraction layer. With onePK:

- Create new or enhance existing applications and services
- Orchestrate, manage, automate, control, and scale your current ones
- Extend network data via APIs to new platform layers
- onePK will be available in limited trial and to early adopters soon.

Languages You Love, Tools of Choice

The new API sets in onePK enable access to consistent features and functionality across Cisco routers, switches, servers, and more. Use the language and tools that work best for you or the project you're working on. Extend the data that your business needs from your network to new abstraction layers to improve usability, flexibility and develop applications and services faster than before. A listing to the solutions included in this category offering as well as links to the detailed descriptions can be found below:

- **onePK: Your Network, Your Way** — Discover what's new with Cisco onePK, which helps deliver consistency of features across Cisco platforms, modular components, and more.
  - Get Details.
- **Cisco IOS Software** — Integrate technology, business-critical services, and hardware support with this network infrastructure software used around the world.
  - Get Details.
- **Cisco IOS XE Software** — The evolution of Cisco IOS Software and IOS XE Software is optimal for facilitating enterprise and service provider services.
  - Get Details.
- **Cisco IOS XR Software** — This self-healing, self-defending, always-on operating system provides service providers a foundation for network and service convergence.
  - Get Details.
- **Cisco NX-OS Software** — This full-featured, modular, and scalable operating system offers high availability, simplified operations, and exceptional flexibility.
  - Get Details.

5.2.2.1 Network Management and Automation — Software products and solutions for data center automation, cloud computing, and IT systems management.

Cisco Response:

Cisco cloud and systems management software solutions are optimized to support innovative Cisco architectures, including:

- Cloud computing
- IP next-generation networks
- Collaboration
- Data center infrastructure
- Video.

The primary goal of Cisco cloud and systems management is to simplify and automate the tasks and operations associated with Cisco equipment.

Cisco's cloud management software enables highly secure, on-demand, and automated IT operations for cloud computing, with policy-based controls for provisioning virtual and physical resources. It includes a self-service portal, orchestration engine, and advanced cloud management capabilities.

Cisco's data center automation products help you better manage your data center operations and applications. You can capture and automate manual tasks across your applications, servers, network, and virtualized infrastructures. Cisco is offering our Cisco Prime for IT and UCS Director solutions for this category. A listing of the solutions offered in this category as well as links to the detailed descriptions can be found below.

The Cisco Prime for IT portfolio of products and solutions helps simplify the deployment and management of Cisco services, technologies, and platforms. The strategy supports integrated lifecycle management of the networks, services, and endpoints for borderless networks, data center, and collaboration architectures. It helps WSCA customers:

- Reduce errors and downtime, automate troubleshooting, and improve the delivery of services
- Speed deployments, minimize IT staffing, and reduce training requirements
- Make the most of network investments through converged management.

IT Product Portfolio

The Cisco Prime product portfolio delivers integrated management solutions that support the convergence of networks, technologies, and services. The product portfolio includes the following.

Cisco Prime Infrastructure

- **Cisco Prime Infrastructure:** Offers comprehensive lifecycle management of wired/wireless access, campus, and branch networks, rich visibility into end-user connectivity, and application performance assurance.
- **Cisco Prime Network Analysis Module (NAM):** Provides deep application-aware network visibility and granular performance analytics that empower network administrators to rapidly isolate and remediate problems and improve the user experience.
- **Cisco Prime Network Registrar:** Provides integrated, scalable, reliable Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and IP Address Management (IPAM) services for both IPv4 and IPv6.

Cisco Prime Collaboration

- Simplified, integrated solution for accelerated provisioning of Cisco Unified Communications users and services and monitoring, troubleshooting, and long-term trending and analytics for Cisco Collaboration voice and video networks.

Data Center

- **Cisco Prime Network Analysis Module**: Provides deep application-aware network visibility and granular performance analytics that empower network administrators to rapidly isolate and remediate problems and improve the user experience.
- **Cisco Netflow Generation Appliance 3240:** Generates, unifies, and exports flow data in high performance data centers, empowering network operations, engineering, and security teams to achieve operational efficiencies, improve services delivery, and harden network security.
- **Cisco Prime Data Center Network Manager:** Combines management of Ethernet and storage networks into a single dashboard to help network and storage administrators troubleshoot health and performance across the whole range of Cisco NX-OS platforms, including the Cisco Nexus and MDS 9000 Families, regardless of protocol type.

Cisco UCS Director

Cisco UCS Director, formerly Cisco Cloupia, delivers unified management for industry-leading converged infrastructure solutions based on Cisco UCS and Cisco Nexus technologies. Cisco UCS Director is a centralized management solution that enables IT departments to experience the full benefits of their converged infrastructure investment by continuing to reduce TCO and save staff time with transparent unified management.

Features and benefits include:

- Provides single interface through which administrators monitor, provision, and manage the system across physical, virtual, and bare-metal environments
- Enables end users to order and deploy new infrastructure instances following IT-prescribed policies and governance
- Uses real-time available capacity, internal policies, and application workload requirements to optimize availability of the most beneficial or best-suited resources
- Shows real-time infrastructure consumption, significantly improving capacity planning and management
- Identifies under-utilized and over-utilized resources
- Supports VMware ESX, Microsoft Hyper-V, and Red Hat hypervisors

- Monitors, manages, and provisions physical, virtual, and bare-metal servers as well as blades
- Delivers policy-based provisioning of physical and virtual switches and dynamic network topologies
- Enables administrators to configure VLANs, virtual Network Interface Cards (vNICs), port groups and port profiles, IP and Dynamic Host Control Protocol (DHCP) allocation, and ACLs across network devices.

Detailed information can be found at: http://www.cisco.com/en/us/products/ps13050/index.html

5.2.2.2 Data Center Management and Automation — Software products and solutions that capture and automate manual tasks across servers, network, applications, and virtualized infrastructure.

Cisco Response:

In this category, Cisco is offering Cisco Prime Data Center Manager (DCNM), UCS Director, and Prime Network Services Director. An overview of the solutions included in this category offering as well as links to the detailed descriptions can be found below.

Cisco Prime Data Center Network Manager is designed to help you efficiently implement, visualize, and manage Cisco Unified Fabric. It includes a comprehensive feature set, along with a customizable dashboard that provides enhanced visibility and Automated Fabric Provisioning of dynamic data centers.

Features and Capabilities

Cisco Prime DCNM provisions and optimizes the overall uptime and reliability of your data center fabric. This advanced management product:

- Provides self-service provisioning of intelligent and scalable fabrics
- Centralizes fabric management to facilitate resource moves, adds, and changes
- Proactively monitors the SAN and LAN, and detects performance degradation
- Opens northbound Application Programming Interfaces (APIs) for Cisco and third-party management and orchestration platforms
- Eases diagnosis and troubleshooting of data center outages
- Simplifies operational management of virtualized data centers.

Primary Benefits of Cisco DCNM

- Offers intuitive, large-scale fabric visualization along with domain views
- Provides cable plan validation and detection
- Features a centralized image and configuration repository
- Communicates with Cisco Prime Network Services Controller for physical and virtual service integration
- Helps you resolve problems faster.

Use Cisco DCNM for technologies such as:

- Cisco virtual PortChannel (vPC)
- Virtual Device Context (VDC)
- Cisco FabricPath
- Fibre Channel over Ethernet (FCoE)
- Fabric zoning and virtual SANs (VSANs).

Simplify Converged Infrastructure Management with Cisco UCS Director

Cisco UCS Director, formerly Cisco Cloupia, delivers unified management for industry-leading converged infrastructure solutions based on Cisco Unified Computing System (UCS) and Cisco Nexus technologies. This unified management supports cohesive, flexible data centers that increase IT and business agility, while reducing operational processes and expenses.

Features and capabilities of Cisco UCS Director include:

Help Reduce Complexity and Costs

A unified management solution enhances the value of converged infrastructure solutions, which bring together computing, networking, and storage resources. These solutions improve IT agility, protect investments, simplify deployment of new services, and optimize asset use. Yet managing each of these layers increases IT complexity and management costs.

Cisco UCS Director reduces the complexity of managing converged infrastructures across physical and virtual resources. It gives you holistic, contextual management, automation, and orchestration across physical, virtual, and bare metal infrastructures, while providing centralized visibility.

Cisco UCS Director delivers effective unified converged infrastructure management through these capabilities:

- Centralized management console, which provides a comprehensive view of the converged infrastructure stack
- Native performance monitoring across all converged infrastructure resources, providing visibility into bottlenecks
- Support for Vblock, FlexPod, and VSPEX, industry-leading converged infrastructure solution brands
- Model-based orchestration capability, for building and executing repeatable workflows without complex custom scripts
- Highly secure management of multi-tenant environments.

If your environment uses converged infrastructures or is considering them, Cisco UCS Director effectively reduces complexity and overall total cost of ownership.

Improve IT Responsiveness and Business Agility

IT needs to maintain complex data centers and deliver new services quickly on tight budgets. By adopting a unified converged infrastructure management solution, your data center will become more flexible and agile, and more responsive to rapidly changing business needs in a timely manner. Unified converged infrastructure management helps you:

- Reduce the effort and time required to manage infrastructure
- Increase the time and budget available to dedicate to new initiatives and services
- Provide greater control over infrastructure resources, so they can be used optimally.

Manage Cloud Network Services with Cisco Prime Network Services Controller

The dynamic nature of cloud environments requires organizations to apply and enforce frequent changes to networks. These networks can consist of thousands of virtual services elements, such as firewalls, load balancers, routers, and switches. Cisco Prime Network Services Controller simplifies operations with centralized, automated multi-device, and policy management.

Features and Capabilities

Cisco Prime Network Services Controller, formerly Cisco Virtual Network Management Center (VNMC), provides centralized multi-device and policy management for Cisco network virtual services. The product addresses the challenge of making frequent changes to complex networks by automating processes,

freeing staff to focus on optimizing the network environment. Cisco Prime Network Services Controller supports greater scalability along with standardization and consistent execution of policies.

When combined with the Cisco Nexus 1000V Switch, Cisco ASA 1000V Cloud Firewall, or the Cisco Virtual Security Gateway (VSG), you can implement the solution to provide:

- Rapid and scalable deployment through dynamic, template-oriented policy management based on security profiles
- Easy operational management through XML APIs to help enable integration with third-party management and orchestration tools
- A non-disruptive administration model that enhances collaboration across security and server teams while maintaining administrative separation and reducing administrative errors.

In addition, support for edge firewalls helps to enable:

- Adding and configuring edge firewalls
- Creating and applying edge security profiles that contain Access Control List (ACL) policy sets (ingress and egress), connection timeout, Network Address Translation (NAT) policy sets, TCP intercept, VPN interface policy sets, and more
- Site-to-site IPsec VPNs.

Improve Security and Enhance Collaboration

Cisco Prime Network Services Controller operates in conjunction with the Cisco Nexus 1000V Virtual Supervisor Module (VSM) to improve operations and collaboration across IT. It streamlines the services performed by security, network, and server administrators.

Security Administrator

With this solution, the security administrator can author and manage security profiles and Cisco Virtual Security Gateway (VSG) instances through the Cisco Prime Network Services Controller programmatic interface with Cisco Nexus 1000V switches. Cisco VSG provides trusted multi-tenant access with granular, zone-based, and context-aware security policies.

Cisco Prime Network Services Controller also manages the Cisco ASA 1000V Cloud Firewall to provide rapid and scalable security at the edge through dynamic, template-oriented policy management.

Network Administrator

The network administrator can author and manage port profiles and Cisco Nexus 1000V virtual switches through the programmatic interface with VMware vCenter.

Server Administrator

The server administrator can select the appropriate port profile in VMware vCenter and associate with an instantiated virtual machine. This can be done through Cisco Prime Network Services Controller XML API support. It facilitates coordination with third-party tools to provision and manage Cisco VSG.

Hybrid Cloud

Cisco Nexus 1000V InterCloud, the network can be more securely extended to the cloud because network and security configurations such as VLANs and policies can be extended.

Using Cisco Prime Network Services Controller, workloads can be migrated from data centers to public clouds, while retaining the same IP addresses and other parameters. This helps avoid the need to redesign the application. Also, workloads in the public cloud can use the same security policies as their counterparts in the data center.

5.2.2.3 Cloud Portal and Automation — Software products and solutions for cloud management with policy-based controls for provisioning virtual and physical resources.

Cisco Response:

Automate IT processes with Cisco Intelligent Automation. These software solutions capture and automate manual tasks across your servers, network, applications, and virtualized infrastructure. By facilitating rapid, precise response to changes in your business and technology, you can:

- Improve effectiveness and reduce risk
- Increase user satisfaction
- Ensure greater return on IT investments.

Use IT Staff Resources More Effectively

Intelligent Automation frees highly skilled IT staff from essential but time-consuming routine maintenance tasks and processes. These tasks are typically 70 to 80 percent of an organization's IT operational expense. With the built-in intelligence of our automation solutions, your IT staff can concentrate instead on innovation, growth, and creating new business value.

Improve Operational Efficiency and Compliance

Intelligent Automation captures best practices, domain knowledge, and analytics, and transforms them into repeatable processes triggered by policy and defined events. These processes improve:

- Efficiency
- Response time
- Compliance
- Visibility
- Business continuity.

Orchestration of Infrastructure and Applications

Cisco Intelligent Automation solutions orchestrate IT infrastructure and application-related processes across the stack. You can:

- Facilitate self-service while enforcing governance and policy-based controls
- Apply abstraction to simplify provisioning of infrastructure and application resources
- Use application events to trigger infrastructure resource changes
- Automate IT processes using best practices to comply with policy and auditability

Intelligent Automation improves efficiency by coordinating the actions of different IT teams and putting capabilities in the hands of the users. An overview of the solutions included in this category offering as well as links to the detailed descriptions can be found below.

Cisco Intelligent Automation for Cloud

- Provides on-demand provisioning and orchestration across compute, network, storage, and applications
- Increases speed, user satisfaction, and operational efficiency in a new cloud-based paradigm.

Learn More

Data Sheets

Cisco UCS Director

- Unifies management across computing, networking, storage, and virtualization layers
- Provides comprehensive management of physical and virtual resources.

Learn More

Data Sheets

Cisco Intelligent Automation for SAP

- Standardizes, unifies, and automates IT processes in complex, heterogeneous SAP environments
- Frees your SAP administration team to deploy and scale automated activities as dictated by your business priorities.

Learn More

Data Sheet

Cisco Tidal Enterprise Scheduler

- Provides a single point of control and visibility for workload automation, by managing and performing all scheduling processes
- Simplifies, automates, and tracks how jobs are carried out.

Learn More

Data Sheets

5.2.2.4 Branch Office Management and Automation — Software products and solutions for management of branch offices. Capabilities include remote troubleshooting, device management, WAN performance monitoring.

Cisco Response:

Cisco is offering our Cisco Prime Infrastructure solution for this category. Cisco Prime Infrastructure accelerates the rollout of unified access services, providing highly secure access and tracking of mobile devices, while assuring application performance and end-user network experience. Cisco Prime Infrastructure couples end-user awareness and performance visibility with lifecycle management of wired and wireless networks for a powerful unified solution.

Feature and Capabilities

Cisco Prime Infrastructure combines the wireless functionality of Cisco Prime Network Control System (NCS) and the wired functionality of Cisco Prime LAN Management Solution (LMS), with rich application performance monitoring and troubleshooting capabilities of Cisco Prime Assurance Manager.

This single solution can enable IT organizations to consolidate tools and converge workflows, reducing operational overhead and increasing productivity. It provides a new operational model based on lifecycle processes aligned with the way network operators do their jobs.

Cisco Prime Infrastructure provides:

- Converged wired and wireless management of access, branch, and wide area networks
- Comprehensive network lifecycle management, including user access visibility, inventory, configuration management, plug and play, radio frequency planning, and best practices reporting
- End-to-end application and service assurance visibility to quickly isolate and troubleshoot performance issues, leveraging technologies, such as flexible NetFlow, Network Based Application Recognition (NBAR), and Medianet Performance Agent
- Prime 360 experience providing a relational, multi-dimensional view of users, applications, and network to simplify the diagnostics and remediation of network and service impacting issues
- Easy deployment and management of Cisco advanced technologies, such as Cisco Adaptive wireless Intrusion Prevention System (wIPS), Cisco CleanAir, VPN, Zone-based Firewall, ScanSafe, and the Cisco Application Visibility and Control (AVC) solutions.

Cisco Prime Infrastructure is built with scalability and extensibility in mind. It has the ability to manage global enterprise networks with thousands of network devices and hundreds of thousands of access devices, or smaller commercial networks with the same level of control and resiliency. It also provides

powerful REST-based APIs enabling IT and service organizations to gather and distribute network information for operations, capacity planning, automation, and business intelligence.

A detailed description of the Cisco Prime Infrastructure solution can be found at: http://www.cisco.com/en/US/products/ps12239/index.html

5.2.3 NETWORK OPTIMIZATION AND ACCELERATION — Devices and tools for increasing data-transfer efficiencies across wide-area networks.

5.2.3.1 Dynamic Load Balancing — An appliance that performs a series of checks and calculations to determine which server can best service each client request in order to select the server that can successfully fulfill the client request and do so in the shortest amount of time without overloading either the server or the server farm as a whole.

Cisco Response:

Cisco NetScaler 1000V is an application delivery controller solution, and part of the Cisco Cloud Network Services architecture. It gives applications critical performance enhancements, including offloading application servers, helping guarantee Quality of Service (QoS), and improving end-user experiences.

Cisco and Citrix Expand Partnership

Companies announce larger virtual networking portfolio and new application delivery controller strategy.

Features and Capabilities

Cisco NetScaler 1000V is a software-based virtual appliance that provides the comprehensive NetScaler feature set.

This easy-to-deploy application delivery solution can be integrated with the overall Cisco Nexus 1000V cloud networking portfolio and run on multiple hypervisor platforms. In this way, it can be deployed on demand, anywhere in the data center, using the Cisco Nexus 1100 Cloud Services Platform or off-the-shelf servers.

The simplicity and flexibility of NetScaler 1000V make it cost effective to fully optimize every web application and more effectively integrate networking services with application delivery.

More Flexible Virtual Form Factor

Virtual services can be more flexibly deployed to cloud service providers without modification. Providers can rely on the same infrastructure and policies that they might have with corresponding physical appliances in their on-premises data centers.

With NetScaler 1000V, customers can have consistency across their physical, virtual, and cloud infrastructures, along with Citrix NetScaler physical appliances.

Integrated with Service Insertion Technology

NetScaler 1000V will be integrated into the Cloud Network Services framework through vPath, and will be an important differentiator against other application delivery controllers (ADCs) products.

vPath is a component of the Cisco Nexus 1000V Virtual Switch. It directs traffic to appropriate virtual service nodes, such as firewalls or ADCs. This is done in the right order for each application, independent of network topology or network services location, and results in greater application mobility and more reliable service delivery.

Reduced Overall Deployment Costs

NetScaler 1000V helps control costs by using processing capacity already in place, including existing virtualized servers and associated resources. Multiple NetScaler 1000V instances can be deployed on a

single server or Cisco Nexus 1100 appliance to optimize hardware infrastructure usage, without creating dependence on specific server hardware.

Detailed information can be found at: http://www.cisco.com/en/us/products/ps13296/index.html

5.2.3.2 WAN Acceleration — Appliance that optimizes bandwidth to improve the end user's experience on a wide area network (WAN). Capabilities should include:

- CIFS acceleration
- Data Compression
- SSL encryption/decryption for acceleration (Optional)
- Layer 4-7 visibility
- Application Specific optimization

Cisco Response:

Cisco WAAS is a software- and hardware-integrated, cloud-ready WAN optimization and application acceleration solution. WAAS appliances offer outstanding deployment scalability and design flexibility, while WAAS software delivers best-in-class application acceleration for the enterprise network.

Jointly validated and supported by leading applications vendors, Cisco WAAS is a cloud-ready and Citrix-ready solution with flexible deployment options: physical appliance, virtual appliance, router-integrated service module, or router-integrated Cisco IOS Software.

Cisco WAAS Software features/benefits include:

- Transparent and standards-based secure application delivery
- LAN-like application performance with application-specific protocol acceleration
- IT agility through reduction of branch and data center footprint
- Enterprise-wide deployment scalability and design flexibility
- Enhanced end-user experience.

Cisco WAAS software, appliances, and modules deliver optimization with the broadest portfolio in the industry. Listed below are the products offered in this category as well as links to the detailed descriptions:

- Cisco Wide Area Virtualization Engine Appliances
- Cisco Wide Area Application Services (WAAS) Modules for ISR
- Cisco WAAS Express
- Cisco Wide Area Application Services (WAAS) Software
- Cisco Virtual Wide Area Application Services (vWAAS)
- Cisco Wide Area Application Services (WAAS) Mobile.

5.2.3.3 High Availability and Redundancy — Limits any disruption to network uptime should an appliance face unforeseen performance issues. Transparently redistributes workloads to surviving cluster appliances without impacting communication throughout the cluster.

Cisco Response:

High Availability (HA) and redundancy is a requirement that must be incorporated in all levels of network architecture. The Cisco portfolio of products and solutions offered for the WSCA Data Communications catalog can be designed and configured to eliminate all single points of failure. Cisco has incorporated redundancy and fault tolerance into the fans, power, processors, line cards, into many of its products and solutions.

Cisco provides a comprehensive set of virtual networking solutions to simplify management and to more securely scale your enterprise data center for private and hybrid clouds. It extends the network edge to the hypervisor and virtual machines, and provides the foundation for Virtual Network overlays, Cisco Open Network Environment (ONE), and Software Defined Networking (SDN). Cisco is offering our Nexus 1000V, Cisco NetScaler 1000V, and Cisco Nexus 1110 Virtual Services Appliance. An overview of the solutions included the offering for this category as well as links to the detailed descriptions can be found below.

Cisco Virtual Networking is built on the foundation of Cisco Nexus 1000V Switch and is hypervisor-agnostic. The Cisco Nexus 1000V offers distinct advantages, including:

- Extensive virtual network services, built on Cisco vPath advanced service insertion and chaining technology
- Support for a wide range of hypervisor environments, including open source
- Feature and management consistency for easy integration with the physical infrastructure
- Availability in two editions (Essential Edition at no cost, and Advanced Edition)
- Policy management and control by the networking team instead of the server virtualization team (separation of duties).

Use Virtual Networking Services

Cisco Nexus 1000V Port Profiles — The Nexus 1000V extends the concept of referenced configuration through the use of Cisco NX-OS port profiles. It publishes them into the hypervisor management domain, allowing ease of assignment and portability of networking and security policies.

Since the Nexus 1000V is a virtual distributed switch, the policies from the profiles are known and supported across Cisco VPATH v2.0– fundamental architecture component of the Cisco Nexus 1000V. vPath optimizes the use of Layer 4-7 virtual networking services in virtual machine and cloud environments.

Service chaining is supported, providing multiple virtual network services as part of a single traffic flow. For example, simply specify the network policy, and let vPath direct traffic:

- First, through the Cisco ASA 1000V Cloud Firewall for tenant edge security
- Then, through the Cisco Virtual Security Gateway for Nexus 1000V switch for a zoning firewall.

Cisco vPath also works on VXLAN to support movement between servers in different Layer 2 domains. Together, these features promote highly secure policy, application, and service delivery in the cloud.

Hybrid Cloud

The Cisco Nexus 1000V Intercloud more securely connects your enterprise data center virtual networks to cloud service providers. This hybrid cloud approach consists of simplified transparent integration, providing:

- Highly secure Layer 2 networking connectivity for workload mobility
- Deployment of security and application services in the cloud
- Management features for hybrid cloud environments.

Optimize Performance of Virtual Applications with Cisco NetScaler 1000V

Cisco NetScaler 1000V is an application delivery controller solution, and part of the Cisco Cloud Network Services architecture. It gives applications critical performance enhancements, including offloading application servers, helping guarantee QoS, and improving end-user experiences.

Integrated with Service Insertion Technology

NetScaler 1000V will be integrated into the Cloud Network Services framework through vPath, and will be an important differentiator against other Application Delivery Controllers (ADCs) products.

vPath is a component of the Cisco Nexus 1000V Virtual Switch. It directs traffic to appropriate virtual service nodes, such as firewalls or ADCs. This is done in the right order for each application, independent of network topology or network services location, and results in greater application mobility and more reliable service delivery.

Reduced Overall Deployment Costs

NetScaler 1000V helps control costs by using processing capacity already in place, including existing virtualized servers and associated resources. Multiple NetScaler 1000V instances can be deployed on a single server or Cisco Nexus 1100 appliance to optimize hardware infrastructure usage, without creating dependence on specific server hardware.

Get a Comprehensive Virtual Services Platform with the Cisco Nexus 1110

Cisco Nexus 1110 Virtual Services Appliance is a dedicated hardware platform for services critical for a virtualized infrastructure. The following virtual networking services are available for the Cisco Nexus 1110 Virtual Services Appliance family:

- Cisco Nexus 1000V Virtual Supervisor Module (VSM) for VMware vSphere
- Cisco Nexus 1000V Virtual Supervisor Module (VSM) for Hyper-V
- Cisco Virtual Security Gateway for Nexus 1000V Series
- Cisco Virtual Prime Network Analysis Module (NAM)
- Cisco Prime Data Center Network Manager
- Imperva SecureSphere Web Application Firewall.

5.2.4 OPTICAL NETWORKING — High capacity networks based on optical technology and components that provide routing, grooming, and restoration at the wavelength level as well as wavelength based services.

5.2.4.1 Core DWDM (Dense Wavelength Division Multiplexing) Switches — Switches used in systems designed for long haul and ultra long-haul optical networking applications.

Cisco Response:

Features and Capabilities

Cisco ushered optical transport into the modern era with the Multiservice Provisioning Platform (MSPP) and continued its leadership by introducing the industry's first widely deployed Reconfigurable Optical Add/Drop Multiplexer (ROADM) technology. This brought the operational ease of use of the MSPP into Dense Wavelength Division Multiplexing (DWDM) networks.

Cisco ROADM innovation continues into its fourth generation, with the first Single Module ROADM. It combines multi-degree wavelength switching functionality with optical amplification and spectrum analysis in a single slot line card.

In combination with advanced features such as colorless and omnidirectional add/drop, the Cisco ONS 15454 Multiservice Transport Platform (MSTP) provides Wavelength Switched Optical Network (WSON) functionality. This embeds optical layer intelligence directly into optical network elements, to support true wavelength-on-demand services and dynamic restoration.

Gain Flexible Aggregation

Cisco optical transport aggregation solutions integrate packet, SONET, and OTN aggregation and switching into the DWDM transport platform. Customers will realize the benefits of efficient wavelength fill and tight communication among network layers.

Selected on a per-card basis, a mix of Layer 1 services, Time Division Multiplexing (TDM), and packet switching technologies can be deployed where needed. This can meet customer and network requirements, while reducing footprint and simplifying operations. The ONS 15454 MSTP can aggregate services into 2.5, 10, 40, and 100 Gb wavelengths.

Scale to 100 Gb and Beyond

As the optical transport industry consolidates around coherent technology for DWDM transport of 100 Gb services, Cisco has demonstrated a clear position of leadership. Cisco coherent technology, powered by nLight Silicon, promises to scale to even greater densities and higher bit rates, leading to 400 gigabit and terabit transport.

An overview of the solutions included in this category offering as well as links to the detailed descriptions can be found below.

ONS 15454 Multiservice Transport Platform (MSTP)

- Delivers any service type to any network location
- Widely deployed across service provider, enterprise, and government customers
- Features 2- to 8-degree ROADM
- Supports colorless and omnidirectional ROADM for touchless programmability
- Excels in metro, regional, and long-haul applications.

Learn More

Data Sheet

Cisco ONS 15216 Series

- Complete suite of passive components for use in DWDM networks
- Minimizes loss, latency, and cost for simplified data center interconnect applications
- Complements ONS 15454 MSTP ROADM configurations with passive add and drop
- Supports up to 96 channels in the C-band.

Learn More

Data Sheet

5.2.4.2 **Edge Optical Switches** — Provide entry points into the enterprise or service provider core networks.

Cisco Response:

The Cisco CPT System complements the Cisco ONS 15454. The Cisco CPT System is an integrated packet transport platform that allows service providers to deploy new packet transport networks. The Cisco CPT System can also be deployed to introduce new packet capabilities in existing DWDM networks that may be using the Cisco ONS 15454. The Cisco ONS 15454 continues to be the best-in-class ROADM for metro-edge and long-haul DWDM applications.

The Cisco Carrier Packet Transport (CPT) System is the first Packet-Optical Transport System (P-OTS) built on standards-based Multiprotocol Label Switching Transport Profile (MPLS-TP) technology. It unifies both packet and transport technologies, giving service providers a strong foundation for the next generation of transport.

This P-OTS platform supports DWDM, OTN, Ethernet, and MPLS-TP integrated in a single system. And it smoothly interoperates with existing deployed IP MPLS networks.

The Cisco Carrier Packet Transport (CPT) System offers:

- A unique architecture with remote managed satellite units
- A compact, energy-efficient form factor
- Outstanding Gigabit Ethernet and 10 Gigabit Ethernet port density per rack unit
- Integrated A-to-Z management for packet and transport.

Business benefits include:

- Agile service delivery, including business, residential, mobile backhaul, data center, and video services
- Support for existing operational models
- "Pay-as-you-grow" scalability.

Listed below are the products offered for this category as well as links to the detailed description:

- Cisco Carrier Packet Transport (CPT) 600
- Cisco Carrier Packet Transport (CPT) 200
- Cisco Carrier Packet Transport (CPT) 50.

5.2.4.3 Optical Network Management — Provides capabilities to manage the optical network and allows operators to execute end-to-end circuit creation.

Cisco Response:

Cisco Prime Optical provides highly efficient management of the converged IP and optical network from access to core, supporting both legacy TDM and Dense Wavelength Division Multiplexing (DWDM) technologies for efficient delivery of next generation services. Through automated mechanisms for configuration, provisioning, and troubleshooting, Cisco Prime Optical helps operators to efficiently execute end-to-end circuit creation. It can also manage every point within the converged network with unprecedented accuracy and scale.

Features and Capabilities

Cisco Prime Optical is available as a standalone product or as a pre-integrated component of the Cisco Prime Carrier Management solution - a comprehensive suite of network management applications that helps simplify the design, provisioning, and management of carrier-grade networks.

Benefits

- Accelerates time to market of services through automation of network discovery, configuration, provisioning, troubleshooting, and change management
- Improves customer satisfaction through rapid resolution to network issues utilizing advanced diagnostics and real-time Service-Level Agreement (SLA) monitoring
- Reduces both Capital Expenditures (CapEx) and Operating Expenses (OpEx) through pre-integration with the Cisco Prime for IP NGN suite of management applications, as well as standards-based interfaces to third-party applications.

Features

- GUI-based user interface with automated configuration and provisioning
- Support for TDM, Wavelength Switched Optical Networks (WSON), DWDM, and Synchronous Optical Networks Synchronous Digital Hierarchy (SONET/SDH)

- Detailed topology maps with detailed navigation, displaying both optical and packet network devices
- Support for up to 5000 optical network elements
- Redundant software and hardware support for high availability, supporting Linux
- Standards-compliant (CORBA TMF 814 v.3) information model and northbound interface (NBI) for integration
- Support for Linux and Cisco Unified Computing System (Cisco UCS), with embedded Oracle options.

A detailed description of the Cisco Optical Management solution can be found at: http://www.cisco.com/en/us/products/ps11670/index.html

5.2.4.4 IP over DWDM (IPoDWDM) — A device utilized to integrate IP Routers and Switches in the OTN (Optical Transport Network).

Cisco Response:

IP over Dense Wavelength-Division Multiplexing (IPoDWDM) is a technology pioneered by Cisco that delivers superior service flexibility, scalability, and resiliency. It allows carriers to capitalize on increasingly bandwidth-intensive and complex applications for next-generation Internet innovations and collaborative business services.

Enhance Your IP Transport through Innovation

IPoDWDM collapses network layers by tightly integrating DWDM interfaces with the routing platform. This increases efficiency, simplifies management, and accelerates service delivery. Combined with industry-leading omnidirectional and colorless ROADM technology, IPoDWDM reduces service truck rolls, power consumption, and space and cooling requirements.

Numerous providers now use the power of IPoDWDM to distribute video content rapidly and efficiently over an all-IP network. They can provision additional network capacity instantly as demand increases for any-play consumer and managed business services.

The Cisco IPoDWDM solution reduces transport elements, while supporting advanced multilayer features such as proactive protection and control plane interaction, dramatically reducing operating expenses and capital costs.

Benefit from Valuable Product Enhancements

The Cisco IPoDWDM solution features:

- Ultra long haul 100 Gb IPoDWDM capability, using the Cisco CRS 1-Port 100 Gigabit Ethernet Coherent DWDM Interface Module
- 100 Gb coherent regeneration using the single-slot, 100 Gb trunk card on the ONS 15454 Multiservice Transport Platform (MSTP), fully compatible with proactive protection
- Proactive protection on the Cisco ASR 9000 Series 2-Port and 1-Port 100 Gigabit Ethernet Line Cards
- Industry-leading 10 Gb IPoDWDM density on the ASR 9000 Series 36-Port and 24-Port 10 Gigabit Ethernet Line Cards
- Complete Generalized Multiprotocol Label Switching (GMPLS) interoperability between the CRS-3, ASR 9000, and ONS 15454 MSTP.

Listed below are the products included in this category offering as well as links to the detailed descriptions.

- Cisco CRS Carrier Routing System

- Cisco ASR 9000 Series Aggregation Services Routers
- Cisco ONS 15454 Multiservice Transport Platform (MSTP).

5.2.5 ROUTERS — A device that forwards data packets along networks. A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network. Routers are located at gateways, the places where two or more networks connect, and are the critical device that keeps data flowing between networks and keep the networks connected to the Internet.

5.2.5.1 Branch Routers — A multiservice router typically used in branch offices or locations with limited numbers of users and supports flexible configurations/feature. For example: security, VoIP, wan acceleration, etc.

Cisco Response:

Cisco Integrated Services Routers Generation 2 (ISR G2) deliver the enterprise network experience through new video-ready capabilities, service virtualization, and operational excellence.

Optimal Application Experience

Extend the role of the router to an application delivery platform with Cisco Integrated Services Router with Application Experience (ISR-AX). This integrated solution is based on the Cisco ISR Generation 2, and includes Cisco Application Visibility and Control and Cisco Wide Area Application Services. ISR-AX provides application services that deliver business applications faster, reduce bandwidth costs and latency by more than 50 percent, and simplify IT management.

Video-Ready Architecture

Built for video delivery from its foundation, the ISR G2 is a Medianet-compliant solution that promotes greater collaboration with comprehensive media services to branches. Services include Cisco TelePresence, video surveillance, digital signage, and scalable Cisco WebEx and desktop conferencing. The media services engine is a voice-and-video-ready digital signal processor that helps to enable these capabilities in a single module.

Service Virtualization

Cisco Services Ready Engines (SRE) provide new services flexibility, cloud extensibility, and services on demand. They decouple hardware and software so virtual services can be remotely deployed and managed, eliminating service calls.

Operational Excellence

Cisco ISR G2 delivers the greatest savings in total cost of ownership. It provides operational simplicity through:

- A single universal Cisco IOS Software image
- The Cisco Services Ready Engine
- Cisco EnergyWise innovation
- A high degree of investment protection that offers a rapid return on investment.

Listed below are the products included in this category offering as well as links to the detailed descriptions.

- Cisco 4451-X Integrated Services Router
- Interfaces and Modules for Cisco 4400 Series.

Cisco 3900 Series

- 3945 Integrated Services Router
- 3945E Integrated Services Router

- 3925 Integrated Services Router
- 3925E Integrated Services Router.

Interfaces and Modules for 3900 Series

Cisco 2900 Series

- 2951 Integrated Services Router
- 2921 Integrated Services Router
- 2911 Integrated Services Router
- 2901 Integrated Services Router.

Interfaces and Modules for 2900 Series

Cisco 1900 Series

- 1941 Integrated Services Router
- 1941W Integrated Services Router
- 1921 Integrated Services Router.

Interfaces and Modules for 1900 Series

Cisco 890, 880, 860 Series

- 892 Integrated Services Router
- 891 Integrated Services Router
- 888 Integrated Services Router
- 887VA-W Integrated Services Router
- 887VA Integrated Services Router
- 887V Integrated Services Router
- 887 Integrated Services Router
- 886VA-W Integrated Services Router
- 886VA Integrated Services Router
- 886 Integrated Services Router
- C881W Integrated Services Router
- 881 Integrated Services Router
- 880 3G Integrated Services Router
- 867 Integrated Services Router
- 861 Integrated Services Router.

5.2.5.2 **Network Edge Routers** — A specialized router residing at the edge or boundary of a network. This router ensures the connectivity of its network with external networks, a wide area network or the Internet. An edge router uses an External Border Gateway Protocol, which is used extensively over the Internet to provide connectivity with remote networks.

Cisco Response:

Transform your Network Edge to deliver high-performance, highly secure, and reliable services to unite campus, data center, and branch networks. Listed below are the products included in this category offering as well as links to the detailed descriptions.

ASR 1000 Series Aggregation Services Router

- Industry-leading performance, service capabilities, and reliability
- Ideal for enterprises for private WAN, Internet edge, and WAN aggregation
- Highly secure, high-performance, instant-on services
- Extends network as a platform for cloud computing.

Learn More

Data Sheets

Catalyst 6500 Series Switch

- WAN service modules facilitate LAN/WAN consolidation
- Advanced traffic management boosts performance and productivity
- Integrated security services protect critical resources and connected users
- Extensible systems readily adapt to new business and IT demands.

Learn More

Data Sheets

5.2.5.3 **Core Routers** - High performance, high speed, low latency routers that enable Enterprises to deliver a suite of data, voice, and video services to enable next-generation applications such as IPTV and Video on Demand (VoD), and Software as a Service (SaaS).

Cisco Response:

Cisco is offering our Carrier Routing System (CRS-X) and our ASR 9000 Series Aggregation Services Routers for this category. A listing of the solutions offered in this category as well as links to the detailed descriptions can be found below.

Cisco Carrier Routing System

The CRS-X provides outstanding economical scale, IP and optical network convergence, and a proven architecture that has delivered 10 times the capacity over 10 years. It offers advanced services intelligence, an environmentally aware design, and system longevity. Furthermore, the CRS-X uses Cisco IOS XR Software, a unique self-healing and distributed operating system.

Features and Capabilities

With an elastic core that is intelligent, programmable, and scalable. The Cisco Carrier Routing System (CRS-X), can:

- Deliver continuous operations at 400 Gbps per slot
- Offer industry-leading scale from a single chassis to a multi-chassis system
- Support 100G speeds and beyond using programmable Cisco nLight Technology
- Combine intelligent IP, lean core transit, and optical transport services
- Improve network monetization through intelligent Layer 4-7 services.

Additional details about the Cisco CRS-X can be found at:
http://www.cisco.com/en/us/products/ps5763/prod_models_comparison.html

The Cisco ASR 9000 Series Aggregation Services Routers can serve as the foundational baseline for next-generation Carrier Ethernet networks, providing up to 96 terabits (tbps) per system.

Cisco ASR 9000

Cisco is evolving its service provider architecture to deliver capabilities for the Next-Generation Internet, which must be more mobile, more visual, more virtual, and yet simpler to manage. This architecture will allow customers to:

- Optimize network performance and efficiency
- Reduce operational costs and complexity
- Enhance customer experiences.

Simplify the Network

The Cisco ASR 9000 system incorporates innovative technologies such as Cisco Network Virtualization (nV) technology, which intelligently blends the edge, aggregation, and access points to simplify operation and accelerate IPv6 services. Two new nV enabled platforms provide additional flexibility and support to optimize service delivery.

The Cisco ASR 903 Series Aggregation Services Routers are ideal for sites requiring high performance with full redundancy in a compact footprint. The Cisco ASR 901 Series Aggregation Services Routers offer very low power consumption at cell sites for mobile backhaul applications.

Working together, the components of Cisco ASR 9000 system can provide the network scale needed to deliver new mobile Internet services while minimizing operational complexity.

Flexible Service Delivery and System Resiliency

The Cisco ASR 9000 Series is a true carrier-class solution. It features the modular, microkernel-based Cisco IOS XR Software operating system, comprehensive system redundancy, and a full complement of network resiliency schemes. It also offers a unique service- and application-level intelligence that focuses on optimized video delivery and mobile Internet.

Cisco ASR 9000 Series routers are equipped with the support of a full set of service activation and provisioning systems. These systems are designed to simplify and enhance the operational and deployment aspects of service-delivery networks, including:

- Business Layer 2 VPN and Layer 3 VPN services
- Mobile aggregation
- Video service-delivery networks.

Additional details about the Cisco ASR 9000 can be found at:
http://www.cisco.com/en/US/products/ps9853/index.html

5.2.5.4 **Service Aggregation Routers** — Provides multiservice adaptation, aggregation and routing for Ethernet and IP/MPLS networks to enable service providers and enterprise edge networks simultaneously host resource-intensive integrated data, voice and video business and consumer services.

Cisco Response:

The Cisco Service Aggregation Routers offered for this category transform the service provider and enterprise network edge by delivering industry-leading performance, instant-on service capabilities, and high availability in a compact form factor. Listed below are the products included in this category offering as well as links to the detailed descriptions.

- Cisco ASR 9000 Series Aggregation Services Routers
- Cisco ASR 1000 Series Aggregation Services Routers
- Cisco ASR 903 Series Aggregation Services Routers
- Cisco ASR 901 Series Aggregation Services Routers

- Cisco ASR 901S Series Aggregation Services Routers
- Cisco XR 12000 Series Router.

5.2.5.5 Carrier Ethernet Routers — High performance routers that enable service providers to deliver a suite of data, voice, and video services to enable next-generation applications such as IPTV, Video on Demand (VoD), and Software as a Service (SaaS).

Cisco Response:

Cisco's Carrier Ethernet system is a proven end-to-end network solution for video, mobile, and cloud. Cisco Carrier Ethernet is a foundational element of the Cisco IP NGN. It helps service providers develop a truly integrated, multidirectional network infrastructure in which all elements, from the core to the edge, access and aggregation, and data center, are intelligently linked and orchestrated to work together.

The Cisco Carrier Ethernet System in the Cisco IP NGN architecture provides integrated links between service- and application-layer components. With the Carrier Ethernet System, customers can:

- Offer highly reliable, end-to-end packet transport that is Cisco test certified and validated
- Extend Multiprotocol Label Switching (MPLS) leadership end-to-end to help enable a single control plane
- Deliver a comprehensive, multimedia service experience anytime, anywhere, and to any Internet-enabled device
- Take full advantage of a unified network management framework designed for the IP NGN.

Listed below are the products included in this category offering as well as links to the detailed descriptions.

- Cisco ME 3400e Series Ethernet Access Switches
- Cisco ME 3600x Series Ethernet Access Switches
- Cisco ME 3800x Series Carrier Ethernet Switch Routers
- Cisco ASR 901 Series Aggregation Services Routers
- Cisco ASR 903 Series Aggregation Services Routers
- Cisco ASR 1000 Series Aggregation Services Routers
- Cisco ASR 9000 Series Aggregation Services Routers
- Cisco ONS 15454 M2 And Cisco ONS 15454 M6
- Cisco Carrier Routing System
- Cisco Catalyst 4500 Series Switches
- Cisco 7600 Series Routers
- Cisco Carrier Packet Transport (CPT) System
- Cisco DCM Series D9901 Digital Content Manager (DCM) IP Video Gateway.

5.2.6 SECURITY

Cisco Response:

Today's borderless organizations are changing, and facing unprecedented challenges. Ever-increasing consumer IT offerings and growing numbers of workers using mobile technology (both in and out of the office) bring new capabilities, along with new security threats. Network guests, contractors, employees, and partners all need differing levels of access. At the same time hackers, botnets, spam, phishing and Trojan viruses present their own issues.

Strengthen Borderless Security with SecureX Architecture

The Cisco SecureX Architecture offers consistent, distributed policy enforcement to provide many facets of protection, from the mobile worker to the virtualized data center. At the core of SecureX is context-aware security that delivers:

- Deeper insight
- More effective security
- Improved operational efficiency.

Context-aware security uses high-level policies that determine who gets access to what type of content, from where, when, and using what application and device.

Cisco solutions and services, such as Cisco TRUSTsec, AnyConnect, Cisco Adaptive Security Appliance (ASA), and Security Intelligence Operations (SIO), provide critical intelligence, policy governance, and enforcement capabilities. They significantly enhance the accuracy, effectiveness, and timeliness of any organization's security implementation.

Advantages of the Cisco SecureX Architecture include:

- Reduced risk; it rapidly identifies and responds to evolving threats
- Better compliance; it enforces business policies and best practices
- Reduced OPEX; it improves efficiency, while reducing complexity and cost
- Better visibility; it adapts to new threats as they happen
- End-to-end coverage, with security embedded in every product in the network
- Award-winning, 24-hour support.

A detailed description of Cisco's end-to-end security portfolio can be found at: http://www.cisco.com/en/us/products/hw/vpndevc/products.html

5.2.6.1 Data Center and Virtualization Security Products and Appliances — Products designed to protect high-value data and data center resources with threat defense and policy control.

Cisco Response:

The Cisco SecureX Architecture features security embedded in the very fabric of the borderless network. Network appliances, Internet scan sensors, and client devices feed real-time data into Cisco Security Intelligence Operations (SIO). This provides global threat correlation and reputation services.

With this architecture, security policies are defined not in the simple terms of ports and addresses, but rather in a higher level, context-aware security policy language that "knows" the identity of user, his or her role in the organization, security posture, and device type. With this information, it can enable the network to grant appropriate access. Cisco security comes in a variety of forms, including:

- Virtual
- Cloud-based
- Appliance
- Modules
- Software for routers and switches.

For added security, you can choose from services such as Security Intelligence Operations and IntelliShield Alerts. Professional services, such as installation, configuration, and ongoing monitoring and threat response, are also available.

Our security products include the most widely deployed firewall in the world, the Cisco Adaptive Security Appliance (ASA), as well as highly secure routers and switches, web security appliances, email security

appliances, Security as a Service, end-point security, VPN clients, and a variety of other security appliances and products.

Cisco security innovations provide highly secure firewall, web, and email services while helping to enable mobility and teleworking. Listed below are the products included in this category offering as well as links to the detailed descriptions.

- Access Control and Policy
- Email Security
- Firewalls
- Intrusion Prevention System (IPS)
- Multi-Function Security
- Network Security
- Security Management
- Small Business Security
- VPN and Endpoint Security Clients
- Web Security.

Access Control and Policy

- Cisco Access Registrar
- Cisco Identity Services Engine.

Identity Services Engine

- Cisco Identity Services Engine (ISE) 3300 Series Appliances.

Network Admission Control

- Cisco NAC Appliance (Clean Access)
- Cisco NAC Guest Server
- Cisco NAC Profiler
- Cisco Trust Agent.

Policy and Access Management

- Cisco Secure Access Control Server for Windows
- Cisco Secure Access Control Server Solution Engine
- Cisco Policy Administration Point
- Cisco Policy Decision Point
- Cisco Policy Enforcement Point
- Cisco Secure Access Control System.

Email Security

- Cisco Cloud Email Security
- Cisco Email Encryption
- Cisco Email Security Appliance.

Firewalls

Adaptive Security Appliances (ASA)

- Cisco Adaptive Security Appliance (ASA) Software
- Cisco ASA 5500-X Series Next-Generation Firewalls
- Cisco ASA 1000v Cloud Firewall
- Cisco ASA Next-Generation Firewall Services
- Cisco PIX Firewall Software.

Firewall Integrated Switch/Router Services

- Cisco Catalyst 6500 Series Firewall Services Module
- Cisco IOS Firewall.

Firewall Management

- Cisco Adaptive Security Device Manager
- Cisco Security Manager.

intrusion Prevention System (IPS)

IDS Integrated Switch/Router Services

- Cisco Catalyst 6500 Series Intrusion Detection System (IDSM-2) Module
- Cisco Integrated Services Routers Intrusion Prevention System Module.

IPS Appliances

- Cisco ASA 5500-X Series Next-Generation Firewalls
- Cisco Intrusion Prevention System
- Cisco IPS 4500 Series Sensors
- Cisco IPS 4300 Series Sensors
- Cisco IPS 4200 Series Sensors.

IPS Management

- Cisco IPS Manager Express
- Cisco Network Traffic Analyst
- Cisco Security Manager.

IPS Modules for ASA

- Cisco ASA Advanced Inspection and Prevention Security Services Module.

Multi-Function Security

Multi-Function Security Appliances

- Cisco Small Business SA500 Series Security Appliances.

Network Security

Integrated Router Security

- Router Security
- Cisco Small Business SA500 Series Security Appliances
- Cisco VPN Internal Service Module for ISR G2.

Integrated Switch Security

- Cisco 7600 Series/Catalyst 6500 Series IPSEC VPN Shared Port Adapter
- Cisco Catalyst 6500 Series Firewall Services Module.

Integrated Threat Control

- Cisco Automated IOS Protection Solution
- Cisco IOS Content Filtering
- Cisco IOS Firewall
- Cisco IOS Flexible Packet Matching (FPM)
- Cisco IOS Intrusion Prevention System (IPS)
- Cisco IOS Network Address Translation (NAT)
- Cisco IOS Network Foundation Protection (NFP).

Security Management

- Cisco Adaptive Security Device Manager
- Cisco Content Security Management Appliance
- Cisco Prime Security Manager
- Cisco Security Manager.

Management Applications

- Cisco IPS Manager Express.

Small Business Security

- Cisco Small Business ISA500 Series Integrated Security Appliances.

VPN and Endpoint Security Clients

Cisco VPN Clients

- Cisco AnyConnect Secure Mobility Client
- Cisco Easy VPN.

IOS VPN

- Dynamic Multipoint VPN (DMVPN)
- Group Encrypted Transport VPN
- Cisco IOS Easy VPN
- Cisco IOS SSLVPN.

VPN Appliances

- Cisco ASA 5500-X Series Next-Generation Firewalls.

VPN Integrated Switch/Router Services

- Cisco 7300 Series Routers
- Cisco 7200 Series Routers
- Cisco 3800 Series Integrated Services Routers
- Cisco 2800 Series Integrated Services Routers
- Cisco 1800 Series Integrated Services Routers
- Cisco 800 Series Routers
- Cisco Catalyst 6500 Series/7600 Series WebVPN Services Module.

VPN Management

- Cisco Adaptive Security Device Manager
- Cisco Security Manager.

Web Security

- Cisco Cloud Web Security
- Cisco Web Security Appliance.

5.2.6.2 **Intrusion Detection/Protection and Firewall Appliances** — Provide comprehensive inline network firewall security from worms, Trojans, spyware, key loggers, and other malware. This includes Next-Generation Firewalls (NGFW), which offer a wire-speed integrated network platform that performs deep inspection of traffic and blocking of attacks. Intrusion Detection/Protection and Firewall Appliances should provide:

- Non-disruptive in-line bump-in-the-wire configuration
- Standard first-generation firewall capabilities, e.g., network-address translation (NAT), stateful protocol inspection (SPI) and virtual private networking (VPN), etc.
- Application awareness, full stack visibility and granular control
- Capability to incorporate information from outside the firewall, e.g., directory-based policy, blacklists, white lists, etc.
- Upgrade path to include future information feeds and security threats
- SSL decryption to enable identifying undesirable encrypted applications (Optional)

Cisco Response:

Cisco Intrusion Prevention Systems (IPS) solutions provide protection against sophisticated threats such as:

- Targeted attacks
- Adaptive Persistent Threats (APTs)
- Botnets
- SQL injection attacks
- Malware targeting application and OS vulnerabilities.

Solutions are available as:

- Dedicated IPS appliances, the Cisco IPS 4300 and 4500 Series Sensors
- Integrated IPS services for the Cisco Adaptive Security Appliances (ASA)

- Hardware modules for Cisco Integrated Services Routers (ISR) and Cisco Catalyst Switches
- Cisco IOS software-based solutions for ISR routers.

Powerful Capabilities for Regulatory Compliance

Cisco IPS solutions can help organizations meet requirements such as:

- PCI Data Security Standard (PCI DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Sarbanes - Oxley Act (SOX)
- Gramm-Leach-Bliley Act (GLBA)
- Federal Information Security Management Act (FISMA).

Simplified Management

Management options for Cisco IPS solutions include IPS Manager Express, a powerful yet easy to use GUI-based management platform for smaller deployments.

For enterprise deployment, Cisco offers Cisco Security Manager.

Advanced Features

Cisco IPS solutions, including the 4300 and 4500 Series IPS Sensors, and the Cisco ASA IPS Solutions, are part of the Cisco SecureX security architecture.

Exclusive Cisco Technology to Block Threats

More than 700,000 Cisco network devices worldwide send current threat information into Cisco Security Intelligence Operations (SIO). The data is analyzed, correlated, and pushed back to devices worldwide as reputation data and outbreak filters. Contain threats and block malware, including zero-day exploits, with these constant updates. Listed below are the products included in this category offering as well as links to the detailed descriptions.

- Cisco IPS Industrial Control Protection
- Cisco ASA 5500 Series IPS Solution
- Cisco IPS 4500 Series Sensors
- Cisco IPS 4300 Series Sensors
- Cisco IPS 4200 Series Sensors
- Cisco Catalyst 6500 Series Intrusion Detection System (IDSM-2) Module
- Cisco IOS Intrusion Prevention System (IPS)
- Cisco Integrated Services Routers Intrusion Prevention System Module.

5.2.6.3 Logging Appliances and Analysis Tools — Solutions utilized to collect, classify, analyze, and securely store log messages.

Cisco Response:

Managing Network Security solutions is often challenging. Accomplishing this in the changing landscape of mobile workers, virtual data centers, and cloud computing-based services adds more complexity.

To address these challenges, Cisco offers centralized operational tools, such as enterprise-grade Cisco Security Manager, to simplify and help you manage your entire Cisco network security deployment.

In addition, Cisco partnered with best-in-class technology vendors to deliver Security Information and Event Management (SIEM) Systems that have been pre-tested and validated with Cisco security products.

This variety of management options give you the flexibility to choose the network security management solutions best suited to your environment and business needs.

Explore and choose from these Cisco and partner security offerings to find the products and services that meet your requirements.

Listed below are the products included in this category offering as well as links to the detailed descriptions.

- Cisco Identity Services Engine
- Cisco Adaptive Security Device Manager
- Cisco Content Security Management Appliance.

Management Applications

- Cisco IPS Manager Express
- Cisco Prime Security Manager
- Cisco Security Manager.

5.2.6.4 Secure Edge and Branch Integrated Security Products — Network security, VPN, and intrusion prevention for branches and the network edge. Products typically consist of appliances or routers.

Cisco Response:

Protect your network by blending stateful inspection and next-generation firewall capabilities with integrated network security services - for security without compromise.

Listed below are the products included in this category offering as well as links to the detailed descriptions.

Cisco ASA 5500 and 5500-X Series Next-Generation Firewalls

- Blends enterprise-class stateful inspection and next-generation firewall capabilities
- Integrates comprehensive next-generation network security services
- Uses a proven, enterprise-class platform
- Available in a wide range of sizes and form factors.

Cisco ASA Next-Generation Firewall Services

- Provides end-to-end network intelligence
- Enables granular control over applications and micro-applications
- Benefits from proactive threat protection updated in near real-time
- Enforces differentiated policies based on the user, device, role, and application type.

Cisco Intrusion Prevention System

- Identifies and stops malicious traffic, worms, viruses, and application abuse
- Delivers intelligent threat detection and protection
- Uses reputation filtering and global inspection to prevent threats
- Promotes business continuity and helps meet compliance needs.

Integrated Security On the ISR G2

- Delivers firewall, intrusion prevention, VPN, and content filtering
- Promotes integrating new network security features on existing routers

- Maximizes network security without adding hardware
- Decreases ongoing support and manageability costs.

Cisco Meraki MX Cloud Managed Security Appliances

- Unified Threat Management (UTM) with networking, security, and application control
- Built-in, centralized cloud management
- Auto VPN provisions site-to-site VPN with a few simple clicks
- Includes WAN optimization, link bonding, Layer 7 firewall, IDS, and more.

5.2.6.5 **Secure Mobility Products** — Delivers secure, scalable access to corporate applications across multiple mobile devices.

Cisco Response:

Get more secure mobile connectivity with SSL VPN (TLS and DTLS), IPSec, IPv4, IPv6 over IPv4 tunneling, web security, and network access manager.

Listed below are the products included in this category offering as well as links to the detailed descriptions.

VPN Services for Cisco ASA Series

- Provides remote access for up to 10,000 SSL or true IPSec connections
- Supports functionality unavailable to a clientless, browser-based VPN connection
- Connects users to IPv6 resources over IPv4 network tunnels
- Facilitates creating user profiles and defining names and addresses of host.

Cisco AnyConnect Secure Mobility Solutions

- Provides an intelligent, smooth, and reliable connectivity experience
- Gives users a choice of how, when, and where they access their information
- Provides remote-access connectivity that is comprehensive and preemptive
- Enforces context-aware policy, and protection from malware.

5.2.6.6 **Encryption Appliances** — A network security device that applies crypto services at the network transfer layer - above the data link level, but below the application level.

Cisco Response:

Meet escalating security and performance requirements with the new algorithms and protocols for encryption, authentication, digital signatures, and key exchange in Cisco Next-Generation Encryption (NGE).

Many of the algorithms that are currently in extensive use cannot effectively scale to meet today's changing security and performance needs. For example:

- RSA signatures and Diffie-Helman (DH) key exchange are increasingly inefficient as security levels rise
- Cipher Block Chaining (CBC) encryption performs poorly at high data rates
- IPSec VPNs use numerous component algorithms, limiting security to the lowest security level of each component.

What you need is the complete algorithm suite in Cisco NGE. In this suite, each component provides a consistently high level of security, and can effectively scale to high throughput and large numbers of connections.

Advances in Cryptography

Cisco NGE technology offers a complete algorithm by using:

- Elliptic Curve Cryptography (ECC) to replace RSA and DH
- Galois/Counter Mode (GCM) of the ADVANCED ENCRYPTION STANDARD (AES) block cipher for high-speed authenticated encryption
- SHA-2 for Hashing operations to replace MD5 and SHA-1.

The algorithms that make up NGE are the result of more than 30 years of global advances and evolution in cryptography. Each component of NGE has its own history, depicting the diverse history of the NGE algorithms, and their longstanding academic and community review. NGE comprises globally created, globally reviewed, and publicly available algorithms.

"Suite B" Algorithms

The U.S. National Security Agency (NSA) has also identified a set of cryptographic standards for public networks. Together, these algorithms are the preferred method to help ensure the security and integrity of information passed over public networks such as the Internet. The NSA calls this set of algorithms "Suite B," and several of these algorithms are also used in NGE.

In addition, NGE algorithms are integrated into IETF, IEEE, and other international standards. As a result, NGE algorithms have been applied to the most recent and highly secure protocols for protecting user data, such as Internet Key Exchange Version 2 (IKEv2) Transport Layer Security (TLS) Version 1.2.

Listed below are the products included in this category offering as well as links to the detailed descriptions.

- Cisco ASA Security Appliance
- Cisco Integrated Services Router (ISR)
  - IPSec VPN and SSL VPN, and VPN Internal Service Module (VPN ISM)
- Cisco ASR 1000 Series.

5.2.6.7 On-premise and Cloud-based services for Web and/or Email Security — Solutions that provide threat protection, data loss prevention, message level encryption, acceptable use and application control capabilities to secure web and email communications.

Cisco Response:

Cisco cloud security offerings help customers take a strategic and architectural approach to cloud adoption. Cisco cloud security solutions dovetail with Cisco data center and Borderless Networks services to deliver high performance and operational simplicity. Cisco cloud security solutions comprise three key areas:

1. In-depth capabilities to help public cloud service providers, subscribers, and private/hybrid cloud practitioners secure their cloud infrastructure
2. Cloud-based email, web, and threat intelligence security for customers
3. Secure cloud access capabilities to help organizations better control access to SaaS applications and to enable a trusted cloud environment.

As WSCA customers embark on their cloud journey, Cisco cloud security helps them reduce their risks with consistent policies and enforcement, up-to-date threat intelligence, greater scalability, and improved performance. Cisco cloud security, in collaboration with many industry partners, helps remove cloud barriers so that customers can achieve the economies of scale and efficiency of cloud computing.

Listed below are the products included in this category offering as well as links to the detailed descriptions.

- Cisco ASA 5500 Series Adaptive Security Appliances: http://www.cisco.com/go/asa
- Cisco AnyConnect: http://www.cisco.com/en/us/netsol/ns1049/index.html
- Cisco Cloud Security: http://www.cisco.com/en/us/netsol/ns1066/index.html
- Cisco Identity Services Engine: http://www.cisco.com/go/ise
- Cisco secure virtual applications and data centers: http://www.cisco.com/en/us/solutions/collateral/ns340/ns517/ns224/ns1097/white_paper_c11-652663.html
- Cisco ScanSafe: http://www.cisco.com/go/scansafe
- Cisco TrustSec: http://www.cisco.com/go/trustsec
- Cisco Virtualization Security: http://www.cisco.com/go/vsec
- Cisco Virtual Services Gateway: http://www.cisco.com/go/vsg
- Cisco Web Security Appliance
- Cisco Email Security Appliance.

5.2.6.8 **Secure Access** — Products that provide secure access to the network for any device, including personally owned mobile devices (laptops, tablets, and smart phones). Capabilities should include:

- Management visibility for device access
- Self-service on-boarding
- Centralized policy enforcement
- Differentiated access and services
- Device Management

Cisco Response:

Enhance network visibility and control with identity-aware secure access solutions.

Cisco is offering our Identity Services Engine and Cisco Secure Access Control System for this category. Listed below is an overview of the products included in this category offering as well as links to the detailed descriptions.

Cisco Identity Services Engine

Whether you need to support BYOD work practices, or provide more secure access to your data center resources, the Cisco Identity Services Engine (ISE) can help. With this all-in-one enterprise policy control platform, you can reliably enforce compliance, enhance infrastructure security, and simplify service operations.

Product highlights include:

- Simplified BYOD onboarding through self-service registration
- Consistent enforcement of context-based policies across wired and wireless networks
- System-wide visibility showing IT who and what is on the network's wired, wireless, or VPN
- Integrated AAA, profiling, posture, and guest services to simplify deployments and cut costs
- Device identification using ISE-based probes, embedded device sensors, endpoint scanning, and device feed service
- Greater visibility and control of the endpoint with Mobile Device Management solution integration.

Cisco ISE offers the following benefits:

- **Highly secure access** — Combine rigorous identification and enforcement with automated user onboarding for consistent access, control, and compliance
- **Greater worker productivity** — Get consistent and dependable access to services from anywhere and anytime
- **Lower operations costs** — Increase IT staff productivity by automating labor-intensive tasks and simplifying service delivery.

Cisco Secure Access Control System

- Controls network access based on dynamic conditions and attributes
- Meets evolving access requirements with rule-based policies
- Increases compliance with integrated monitoring, reporting, and troubleshooting capabilities
- Takes advantage of built-in integration capabilities and distributed deployment.

5.2.7 STORAGE NETWORKING — High-speed network of shared storage devices connecting different types of storage devices with data servers.

Cisco Response:

Storage costs are growing faster than server costs. Businesses need more efficient, cost-effective, and responsive Storage Area Networks (SANs), without increasing overall power consumption. Also, in today's environments that must comply with government regulations for data recovery, 24-hour access to critical information is imperative.

Cisco SANs provide:

- Multiprotocol storage networking: Achieve lower Total Cost of Ownership (TCO) and greater agility by integrating disparate protocols such as FC, FICON, FCoE, iSCSI, and FCIP
- Unified OS and management tools: Reduce operating expenses and provide operational simplicity, seamless interoperability, and consistent features
- Enterprise-class storage connectivity: Support significantly higher virtualized workloads, to increase availability, scalability, and performance
- Services-oriented SANs: Extend any network service to any device, regardless of protocol, speed, vendor, or location.

Cisco MDS 9000: Flexible, Agile, Cost Effective

With Cisco MDS 9000 Switches, you can optimize physical resources, reduce operating costs such as energy use, and decrease capital expenditures to achieve lower TCO.

With industry-leading features and advanced capabilities, Cisco MDS 9000 Switches continue to be the leading platform for hosting intelligent multilayer services that fill business needs such as:

- SAN consolidation
- Storage encryption
- Disaster recovery
- Data mobility
- SAN security
- Replication.

The MDS 9000 product family also facilitates server storage and fabric virtualization to provide an end-to-end virtualization solution for the data center.

SANs are central to the Cisco Data Center Business Advantage architecture. They provide a networking platform that helps IT departments achieve lower total cost of ownership, enhanced resiliency, and greater agility.

Cisco MDS 9000 Multilayer Directors and Fabric Switches included in this offering as well as links to the detailed descriptions are listed below:

- Cisco Fabric Manager
- Cisco MDS 9700 Series Multilayer Directors
- Cisco MDS 9500 Series Multilayer Directors
- Cisco MDS 9200 Series Multiservice Switches
- Cisco MDS 9100 Series Multilayer Fabric Switches
- Cisco MDS 9000 Intelligent Fabric Applications
- Cisco MDS 9000 NX-OS and SAN-OS Software
- Cisco MDS 9000 Port Analyzer Adapters
- Cisco MDS 9000 SAN Management
- Cisco MDS 9000 Series Multilayer Switches
- Cisco MDS 9000 Services-Oriented SANS
- Cisco MDS 9000 Software Licensing
- Cisco Storage Networking Modules.

5.2.7.1 Director Class SAN (Storage Area Network) Switches and Modules — A scalable, high-performance, and protocol-independent designed primarily to fulfill the role of core switch in a core-edge Fibre Channel (FC), FCOE or similar SAN topology. A Fibre Channel director is, by current convention, a switch with at least 128 ports. It does not differ from a switch in core FC protocol functionality. Fibre Channel directors provide the most reliable, scalable, high-performance foundation for private cloud storage and highly virtualized environments.

Cisco Response:

Adopt intelligent features of a high-performance, multi-protocol switch fabric. Address requirements of large data center environments. An overview of the products included in this offering as well as links to the detailed descriptions are listed below:

- Cisco MDS 9700 Series Multilayer Directors
  - Ready-to-adapt to accommodate future physical, virtual, and cloud environments
  - Up to 384 line rate 2/4/8/16-Gbps Fibre Channel ports
  - Fully redundant components and fault-tolerant design
  - Multi-protocol innovations for architectural flexibility
- Cisco MDS 9500 Series Multilayer Directors
  - Platform for smart storage services
  - Designed for large virtualized data center environments
  - Up to 528 1/2/4/8-Gbps Fibre Channel ports.

5.2.7.2 Fabric and Blade Server Switches — A Fibre Channel switch is a network switch compatible with the Fibre Channel (FC) protocol. It allows the creation of a Fibre Channel fabric, which is currently the core component of most SANs. The fabric is a network of Fibre Channel devices, which allows many-to-many communication, device name lookup, security, and redundancy. FC switches

implement zoning; a mechanism that disables unwanted traffic between certain fabric nodes.

Cisco Response:

Cisco Fibre Channel Blade Switch Overview

Cisco Fibre Channel blade switches are built using the same hardware and software platform as Cisco MDS 9000 Family Fibre Channel switches and hence are consistent in features and performance. Architecturally, blade switches share the same design as the Cisco MDS 9000 Family fabric switches.

Cisco offers Fibre Channel blade switch solutions for HP c-Class BladeSystem and IBM BladeCenter.

- Cisco Fibre Channel Blade Switch for HP c-Class BladeSystem

  The Cisco MDS HP Blade Switch (**Figure 7**) is a Fibre Channel blade switch for HP c-Class BladeSystem. It comes in two models: the base 12-port model and a 24-port model. A 12-port license upgrade is available to upgrade the 12-port model to 24 ports. In the 12-port model, 8 ports are for server connectivity, and 4 ports are for SAN connectivity. In the 24-port model, 16 ports are for server connectivity, and 8 ports are for SAN connectivity.

Figure 7. MDS 9124e FC Blade Switch for HP c-Class BladeSystem

- Cisco Fibre Channel Blade Switch for IBM BladeCenter

  The Cisco MDS IBM Blade Switch (**Figure 8**) is a Fibre Channel blade switch for IBM BladeCenter. It comes in two models: a 10-port switch and a 20-port switch. A 10-port upgrade license is available to upgrade from 10 ports to 20 ports. In the10-port model, 7 ports are for server connectivity, and 3 ports are for SAN connectivity. In the 20-port model, 14 ports are for server connectivity, and 6 ports are for SAN connectivity.

Figure 8. MDS FC Blade Switch for IBM BladeCenter

- Features

  Some of the unique features of the Cisco MDS 9000 Family switches are:

  - Virtual SANs (VSANs): VSANs partition the physical SANs into logical SANs, which can be managed like separate SANs or can consolidate different physical SANs into fewer Fibre Channel switches. Each VSAN can be managed by different administrators using VSAN-aware role-based access control (RBAC). The VSANs can be configured with different traffic priorities to enable service differentiation.
  - Inter-VSAN Routing (IVR): IVR allows sharing of scarce resources among the VSANs while maintaining the isolation between them. IVR increases the utilization of both switches and SAN resources by enabling flexibility of any-to-any connectivity.

- HP c-Class BladeSystem

  The HP c-Class BladeSystem blade chassis is offered in two models: HP c3000 and c7000. The enclosure holds up to 16 servers and 8 interconnect bays for I/O connectivity. Refer to the HP c-Class enclosure specifications for more information about setting up connectivity: http://h18000.www1.hp.com/products/blades/components/enclosures/c-class/.

- IBM BladeCenter

  IBM BladeCenter is built on the IBM System x architecture offered in many models. The enclosure holds up to 14 blades and 4 IO modules. Refer to IBM BladeCenter specification at http://www-03.ibm.com/systems/bladecenter/.

5.2.7.3 Enterprise and Data Center SAN and VSAN (Virtual Storage Area Network) Management — Management tools to provisions, monitors, troubleshoot, and administers SANs and VSANs.

Cisco Response:

You can achieve higher security and greater stability in Fibre Channel fabrics by using Virtual SANs in Cisco MDS SAN-OS. VSANs provide isolation among devices that are physically connected to the same fabric. With VSAN, you can create multiple logical SANs over a common physical infrastructure.

Cisco Prime Data Center Network Manager

Cisco is offering our Prime Data Center Network Manager solution for this category. Cisco DCNM provides a robust framework and comprehensive feature set that meets the routing, switching, and storage administration needs of present and future virtualized data centers. Cisco Prime DCNM offers visibility into the virtualized hosts by integrating with industry standard hypervisors and provides host-tracking capability to easily manage and diagnose virtual and physical servers. Cisco DCNM streamlines the provisioning of the unified fabric and proactively monitors the LAN and SAN components. Offering an exceptional level of visibility and control through a single management pane for the Cisco Nexus, Cisco Unified Computing System, and Cisco MDS 9000 Family products, Cisco DCNM is the Cisco-recommended solution for managing mission-critical data centers. Benefits include:

- Multi-protocol management of storage and Ethernet networks
- Troubleshooting of health and performance of Cisco Nexus and MDS switches
- Simplified wizard and template-based configuration and provisioning
- Dashboard and report-based resource management.

Learn More

Data Sheets

5.2.7.4 SAN Optimization — Tools to help optimize and secure SAN performance (ie. Encryption of data-at-rest, data migration, capacity optimization, data reduction, etc.

Cisco Response:

Optimize your data center resources by providing integrated, high-performance applications to Cisco storage networks. Support disaster recovery, security, data mobility, and other heterogeneous storage requirements, without adding appliances or using host or array resources.

Cisco MDS 9000 Family Services Nodes provide network-hosted services to Cisco storage networks such as SAN extension (FCIP), I/O Acceleration (IOA), XRC Acceleration (XRC), Storage Media Encryption (SME), and Data Mobility Manager (DMM).

Network-assisted applications are enabled through the open Intelligent Services API (ISAPI). Cisco makes this development platform available to original storage manufacturers (OSMs) and independent software vendors (ISVs) who want to develop storage applications on the Cisco storage networks platform.

Storage network administrators will get:

- Flexibility to extend any service to any device in the storage network
- I/O intensive data path processing tasks at wire speed transparent to host and array applications
- Non-disruptive deployment (no SAN reconfiguration or rewiring to insert in-band appliances)
- High performance with dedicated network resources delivering services at wire speed
- Linear scalability through additional modules or switches
- Automatic dual-path load balancing for high availability
- Wizard-based provisioning via the Fabric Manager GUI.

These services are all provided over your MDS network. Listed below are the products included in this offering as well as links to the detailed descriptions:

Hardware

- MDS 9000 16-Port Storage Services Node
- MDS 9000 18/4 Multiservice Module
- MDS 9222i Multiservice Switch.

Software

- Storage Media Encryption
- Data Mobility Manager
- IO Accelerator
- SAN Extension
- Business Continuity and Disaster Recovery.

5.2.8 SWITCHES — Layer 2/3 devices that are used to connect segments of a LAN (local area network) or multiple LANs and to filter and forward packets among them.

5.2.8.1 Campus LAN – Access Switches — Provides initial connectivity for devices to the network and controls user and workgroup access to internetwork resources. The following are some of the features a campus LAN access switch should support:

- Security
  - i. SSHv2 (Secure Shell Version 2)
  - ii. 802.1X (Port Based Network Access Control)
  - iii. Port Security
  - iv. DHCP (Dynamic Host Configuration Protocol) Snooping

- VLANs
- Fast Ethernet/Gigabit Ethernet
- PoE (Power over Ethernet)
- link aggregation
- 10 Gb support
- Port mirroring
- Span Taps
- Support of IPv6 and IPv4
- Standards-based rapid spanning tree
- Netflow Support (Optional).

Cisco Response:

Benefits

2366p010/a

Figure 9. Cisco Access Switch Benefits

Catalyst Access Switches Help You Build a Borderless Business

Cisco Catalyst access switching and wireless LAN solutions, part of the Cisco Borderless Networks architecture, help deliver agile services and applications to manage, secure and govern your network.

Ease of Operations

Cisco access switches allow your network to adapt and support new application deployments to meet changing business needs. A 10-Gigabit upgrade with the Network Module helps with scalability while protecting your existing investments. The switches also support Catalyst Smart Operations features that help automate infrastructure deployment.

Borderless Security

Strengthen your control over wired and wireless access to your network. Cisco access switches provide end-to-end security using identity-based policy and threat intelligence capabilities. TrustSec helps secure networks with policy-based access control while MACSec provides hardware encryption for a higher level of security.

Borderless Experience

Cisco access switching provides the service intelligence and performance required for business-grade video and other revenue-generating services.

Cisco network access makes borderless mobility possible with a unified approach to wired and wireless services, such as location awareness, to enhance application performance. Power over Ethernet Plus helps ensure compatibility with future versions for deployment of next generation high power devices.

Sustainability

Catalyst switching solutions help implement greener practices with measurable power efficiency, integrated services, and Cisco EnergyWise, an innovative technology for company-wide energy management. StackPower on Cisco Catalyst 3750-X Switches provides high-availability and operational efficiency.

When the network knows, your business can fully adapt to dynamic market conditions.

With high availability, both stackable and standalone options, and EnergyWise technology for efficient power management, Catalyst access switches can help you build a borderless business by providing ease of operations, sustainability, borderless experience, and borderless security.

Listed below are the products included in this offering as well as links to the detailed descriptions:

- Cisco Catalyst 4500E Series Switches
- Cisco Catalyst 3850 Series Switches
- Cisco Catalyst 3750-X Series Switches
- Cisco Catalyst 3750-E Series Switches
- Catalyst 3560-X
- Cisco Catalyst 3560-E Series Switches
- Cisco Catalyst 2960-Plus Series Switches
- Cisco Catalyst 2960-S Series Switches
- Cisco Catalyst 2960-SF Series Switches
- Cisco Catalyst 2960-X Series Switches
- Cisco Catalyst 2960 Series Switches
- Cisco Energywise
- Cisco Redundant Power Systems
- Cisco Catalyst 3560-C Series Switches
- Cisco Catalyst 2960-C Series Switches.

5.2.8.2 Campus LAN – Core Switches — Campus core switches are generally used for the campus backbone and are responsible for transporting large amounts of traffic both reliably and quickly. Core switches should provide:

- High bandwidth
- Low latency
- Hot swappable power supplies and fans
- Security
  - i. SSHv2
  - ii. MacSec encryption
  - iii. Role-Based Access Control Lists (ACL)
- Support of IPv6 and IPv4
- 1/10/40/100 Gbps support
- IGP (Interior Gateway Protocol) routing

- EGP (Exterior Gateway Protocol) routing
- VPLS (Virtual Private LAN Service) Support
- VRRP (Virtual Router Redundancy Protocol) Support
- Netflow Support.

Cisco Response:

Cisco Catalyst Switches provide the scale, intelligence, simplicity, and security essential to accelerate business initiatives and protect investments.

Resiliency

High-availability features help ensure nonstop connectivity and business continuity. In-service software upgrades virtually eliminate downtime for updates, while the Virtual Switching System (VSS) enables two active switches to appear as one, with a single point of management.

Consistent Experience

Only Cisco extends consistent network services – for security, video, wireless, network management, and more – from the user edge through campus distribution, core, and the data center. Integrated services modules in Catalyst 6500 Series Switches reduce network footprint and simplify management.

Application Visibility

Cisco Flexible NetFlow technology helps enable customers to view traffic flows granularly to the application level. Greater control over flow data helps speed responses to mitigate attacks, adjust bandwidth provisioning, and enable continuous monitoring.

Simplified Operations

Cisco Catalyst SmartOperations brings together a set of technologies and Cisco IOS Software features to simplify network planning, deployment, monitoring, and troubleshooting, lowering IT operating costs and total cost of ownership.

Descriptions, benefits, and links to the detailed description of the Campus LAN Core switches included in the offering for this category are listed below:

Cisco Catalyst 6800 Series Switches

- Scalable platform optimized for 10/40/100 Gigabit services with higher slot capacity (up to 880 Gigabits) and switching capacity (up to 11.4 Tb)
- Intelligent services with Catalyst 6500 DNA and Cisco One Platform Kit (OnePK) support
- Simplified operations with Catalyst Instant Access
- Highly secure for users and applications with comprehensive wired, wireless, and VPN security.

Learn More

Data Sheets

Cisco Catalyst Instant Access

Benefits include:

- **Single Switch Configuration** — All access switches are configured and managed through the Catalyst 6500 or 6800 series core switch, which saves time and increases efficiency.
- **Consistent Features Campus-wide** — Instant Access helps ensure feature consistency because the access switches and the core switch work as a single extended switch. Network downtime from feature inconsistencies is eliminated.

- Centralized Consistent Security - Security policies are applied on the core switch, which provides a single consistent policy campus-wide or branch-wide. IT can cost effectively comply with regulations.
- **Scaled SDN Deployment** — SDN services can be scaled and quickly deployed because access switches do not have to be configured or programmed individually.
- **Single Software Image Management** — With Instant Access, only the core switch needs software image installation and upgrades. This centralization saves time and helps maintain software image consistency across switches.
- **Faster Service Deployments** — This solution helps IT quickly and easily deploy new services, such as BYOD, IPTV, and guest network. Single-switch qualification and staging also help reduce errors in deployments.

Additional information can be found at: http://www.cisco.com/en/us/netsol/ns1240/index.html#~overview

Cisco Catalyst 6500 Series Switches

- Flagship Catalyst switching services platform for core/distribution deployments
- Virtual Switching System bolsters availability and scales to 4-terabit capacity
- Up to 160 Gigabits per slot; 100 Gigabit Ethernet-ready
- Integrated services modules enhance security, manageability, and wireless control.

Learn More

Data Sheets

Compare Products

Cisco Catalyst 4500E Series Switches

- Catalyst switching platform for moderate density 1 G/10 G distribution deployments
- Up to 848 Gbps switching capacity
- Up to 196 x 1 G SFP ports, up to 100 x 10 G SFP+ ports
- High availability with In-Service Software Upgrade and Stateful Switchover

Learn More

Data Sheets

Compare Products

Cisco Nexus 7000 Series Switches

- Offers highest switching capacity; up to 1.3 terabits per slot, 83+ terabits per chassis
- Provides high 1,10, 40, and 100 Gigabit Ethernet scalability
- Offers the industry's most comprehensive data center feature set
- Delivers advanced services; high availability; hitless In-Service Software Upgrade (ISSU)
- Is ideal for data center access, aggregation, and core deployments.

Learn More

Data Sheets

ASR 9000 Series

- Offers nonstop video, enhanced scalability, and reduced carbon footprint
- Scales up to 96 tbps per system with comprehensive system redundancy
- Offers unique service- and application-level intelligence.

Learn More

Data Sheets

5.2.8.3 Campus Distribution Switches — Collect the data from all the access layer switches and forward it to the core layer switches. Traffic that is generated at Layer 2 on a switched network needs to be managed, or segmented into Virtual Local Area Networks (VLANs), Distribution layer switches provides the inter-VLAN routing functions so that one VLAN can communicate with another on the network. Distribution layer switches provides advanced security policies that can be applied to network traffic using Access Control Lists (ACLs).

- High bandwidth
- Low latency
- Hot swappable power supplies and fans
- Security (SSHv2 and/or 802.1X)
- Support of IPv6 and IPv4
- Jumbo Frames Support
- Dynamic Trunking Protocol (DTP)
- Per-VLAN Rapid Spanning Tree (PVRST+)
- Switch-port auto recovery
- NetFlow Support or equivalent

Cisco Response:

Cisco Catalyst Switches provide the scale, intelligence, simplicity, and security essential to accelerate business initiatives and protect investments. Due to the versatility of the Cisco Catalyst Switch portfolio, the switches in this offering could be utilized as core or distribution based on the size and complexity of the network.

Resiliency

High-availability features help ensure nonstop connectivity and business continuity. In-service software upgrades virtually eliminate downtime for updates, while the Virtual Switching System (VSS) enables two active switches to appear as one, with a single point of management.

Consistent Experience

Only Cisco extends consistent network services – for security, video, wireless, network management, and more – from the user edge through campus distribution, core, and the data center. Integrated services modules in Catalyst 6500 Series Switches reduce network footprint and simplify management.

Application Visibility

Cisco Flexible NetFlow technology helps enable customers to view traffic flows granularly to the application level. Greater control over flow data helps speed responses to mitigate attacks, adjust bandwidth provisioning, and enable continuous monitoring.

Simplified Operations

Cisco Catalyst SmartOperations brings together a set of technologies and Cisco IOS Software features to simplify network planning, deployment, monitoring, and troubleshooting, lowering IT operating costs and total cost of ownership.

Listed below are the products included in this offering as well as links to the detailed descriptions:

- Cisco Catalyst 6800 Series Switches
- Cisco Catalyst 6500 Series Switches
- Cisco Catalyst 4500E Series Switches
- Cisco Catalyst 4500-X Series Switches.

5.2.8.4 Data Center Switches — Data center switches, or Layer 2/3 switches, switch all packets in the data center by switching or routing good ones to their final destinations, and discard unwanted traffic using Access Control Lists (ACLs), all at Gigabit and 10 Gigabit speeds. High availability and modularity differentiates a typical Layer 2/3 switch from a data center switch. Capabilities should include:

- High bandwidth
- Low latency
- Hot swappable power supplies and fans
- Ultra-low latency through wire-speed ports with nanosecond port-to-port latency and hardware-based Inter-Switch Link (ISL) trunking
- Load Balancing across Trunk group able to use packet based load balancing scheme
- Bridging of Fibre Channel SANs and Ethernet fabrics
- Jumbo Frame Support
- Plug and Play Fabric formation that allows a new switch that joins the fabric to automatically become a member
- Ability to remotely disable and enable individual ports
- Support NetFlow or equivalent

Cisco Response:

The Cisco Nexus family of products provides a wide range of business benefits.

Simplified

- Improve efficiency, simplify mobility for physical and virtual machines and services, and provide end-to-end visibility for any topology.
- Significantly speed up workload delivery for both physical and virtual rollouts with network automation and provisioning, and better integration with orchestration, automation tools, and cloud platforms.
- Make troubleshooting easier with centralized fabric management across physical and virtual workloads.

Convergence

Cisco Nexus solutions simplify the data center network by converging LANs and SANs, and by using Data Center Bridging (DCB), Fibre Channel Over Ethernet (FCOE) protocols, and Unified Ports.

- Lower total cost of ownership by up to 50 percent
- Reduce capital expenses through fewer host adapters, switches, and cables

- Cut operational expenses through reduced power, cooling, rack space, and floor space requirements
- Adopt solutions incrementally, without a complete upgrade
- Reduce disruptions to existing management and operations.

Scalability

Cisco Nexus solutions help enterprises scale for the more-complex workloads of virtualization, the proliferation of virtual machines, and the challenges of cloud computing.

- Unify all network locations into one environment
- Support efficient access and use of resources, regardless of size or scope
- Provide resilient, scalable networks with predictable performance and reduced complexity
- Simplify management with fabric extensibility.

Intelligence

Cisco Nexus delivers intelligent services directly into the network fabric. It transparently extends the network to encompass all network locations into a single, extended environment with consistent services and policy.

- Make services available consistently across applications and workloads
- Scale service delivery capability automatically
- Deploy applications faster, with policy-based compliance instead of physical infrastructure changes.

The Cisco Nexus and Catalyst families of switches are designed to meet the stringent requirements of the next-generation data center. Listed below are the products included in this offering as well as links to the detailed descriptions:

- Cisco Nexus 7000 Series Switches
- Cisco Nexus 6000 Series Switches
- Cisco Nexus 5000 Series Switches
- Cisco Nexus 3000 Series Switches
- Cisco Nexus 2000 Series Fabric Extenders
- Cisco Nexus 1100 Series Virtual Services Appliances
- Cisco Nexus 1000V Switch For Vmware Vsphere
- Cisco Nexus 1000V Switch For Microsoft Hyper-V
- Cisco Data Center Network Manager
- Cisco Fabric Manager
- Cisco NX-OS Software.

5.2.8.5 Software Defined Networks (SDN) - Virtualized Switches and Routers — Technology utilized to support software manipulation of hardware for specific use cases.

Cisco Response:

Included in this offering is onePK, Cisco Meraki Cloud-Managed Access Switches, and Cisco Cloud Management. Descriptions, benefits, and links to the detailed description of the SDN products included in the offering for this category are listed below:

Benefits of the Cisco Open Network Environment

Cisco ONE offers a comprehensive vision across all IT infrastructure, flexible deployment options (SDN and non-SDN programming models), and investment protection through incremental adoption. It is the broadest structured approach to open networking in the industry today.

In addition, professional services from Cisco and our partners, plus global support, help ensure long-term success:

- Extending the capabilities of existing, proven validated infrastructure significantly reduces risk and time to capability.
- Cisco ONE is designed to be deployed incrementally, preserving investments and avoiding turnover.
- Cisco ONE builds on Cisco innovation together with industry development of SDN technologies and standards. This approach maintains high flexibility and choice for customers.

The Cisco onePK model is consistent across a wide range of Cisco routers and switches. Organizations and service providers can write their applications once and deploy them anywhere, with investment protection for future platforms. Cisco Certified developer partners can be confident of a large market opportunity that targets a large installed base of network equipment.

The Cisco XNC offers the flexibility of conformance to an open standard and the capability to control third-party network devices, while supporting multiple API and SDN specifications. The industry-leading Cisco VNI forms the foundation for programmable network overlays that can simplify cloud deployments and integrate automation and orchestration tools.

We are in a unique position to help you evaluate these new technologies and determine how best to integrate them into your broader networking strategies. As the industry leader in networking, we have the expertise and experience to help your organization extract tangible value from Cisco ONE to support your strategic goals.

Why Cisco?

Customer Value and Choice; Flexible Deployment Options

- Industry leader: Cisco is the worldwide leader in networking with a deep commitment to open networking including open source, open standards, and open interfaces. We have been contributing to and leading several initiatives for open standards and open source, including at the Open Network Foundation, OpenStack consortium, OpenDaylight project, IETF, I\EEE, and ETSI among others.
- Unparalleled innovation: Only Cisco brings together innovation across hardware, software, services, and ASICs to deliver tightly integrated solutions that offer lower TCO. We have traditionally offered strong investment protection with evolutionary approaches to revolutionary benefits.
- Cross-architectural solutions: Cisco offers holistic cross-architectural solutions that are secure and transcend branch-office, campus, data center, cloud, and service provider environments.
- Choice of deployment models: Cisco offers a use-case led deployment model to embrace emerging technologies such as network programmability and SDN in an evolutionary manner, offering investment protection and lower TCO.
- Technical and Advanced Services: Cisco has a mature partner ecosystem including training and developer partners, the Cisco Development Network (CDN), as well as a Professional and Technical Support Services organization to help foster customer success through all aspects of the customer's open networking and SDN experience. Working together, the Cisco ecosystem helps customers architect software-led programmability to enable simplification in the overall solution.

One Platform Kit (onePK) for Developers

Cisco onePK, short for One Platform Kit, is an easy-to-use developer's toolkit for innovation, automation, and service creation. onePK delivers the benefits of network programmability on Cisco routers and switches. onePK allows you to tie your network more effectively to ever changing application needs, providing improved business agility and decreased OPEX. onePK allows your network's power to be unleashed in new ways for a faster, more flexible, and intelligent infrastructure.

What Problems Does It Help Solve?

- Need for deeper access to information stored within network devices
- Need to exercise greater or more precise control over flows and routes
- Need to extract particular packets for modification and reinjection
- Need to improve quality of service based on custom parameters
- Need to add services to the network without making a huge infrastructure investment
- Need to allow programmers to augment network operation in response to application-specific business logic
- Need to bridge the operational gap between disparate systems
- Need to deploy a gateway or network service without adding hardware or constraining functionality based on physical connectivity.

Applications of onePK for Specific Customer Types

- Improve visibility and control over network operations (all market segments)
- Reduce hardware footprint for new services or gateway functions (enterprise and service provider)
- Automate new service provisioning for customers (cloud service provider)
- Deliver more consistent quality of service to multimedia service customers (service provider)
- Achieve higher levels of data security when transmitting over untrusted networks (government/defense)
- Improve the perceived speed of the application to users of hyper-scale data center services (for example, social media websites)
- Orchestrate new services or additional resources more quickly and cost-effectively (data centers and service providers)
- Modify packets to enhance security, reliability, or performance for customers (data centers and service providers).

One Platform Kit (onePK)

onePK is a flexible development environment that supports C or Java programs. Your source code can be written and compiled using any tools that you want. The onePK infrastructure is built right into the operating system of all Cisco platforms and communicates with the onePK presentation layer, supporting the developer's C or Java programs.

This architecture gives users maximum deployment flexibility. onePK along with Cisco's container support allows the user to host applications on the device processor board, a services blade available with some Cisco platforms or a separate server that communicates to the onePK infrastructure using a secure communications channel.

Because the API is consistent across all Cisco platforms, the developer can write an application once and have that application deployed on any switch or router.

What Are the Benefits of onePK?

- Build, automate, improve: Create new or improve existing applications and services, increase productivity
- Speed and faster adaptability: Provide flexibility for rapidly changing business needs and reduced operating costs
- Extend: Extend the functionality of your network
- New revenue opportunities: Provide monetization of new applications or services, create services more quickly with code that you can write once and run anywhere
- Simplicity, integration, and the power of choice
- Utilize with your programming language and tools of choice
- Run it on any server or right in the network device.

Why Cisco?

The onePK model is consistent across all of the wide variety of Cisco routers and switches. Write your application once and deploy it anywhere. Because it's Cisco, you can be sure that your onePK application will be supported on the widest variety of network devices in the industry. And, if you are a Cisco certified developer partner, onePK gives you the largest market opportunity.

Additional details about the onePK solution can be found at:
http://www.cisco.com/en/US/prod/iosswrel/onepk.html

Cisco Meraki Cloud-Managed Access Switches

Combine the benefits of cloud-based centralized management with a powerful, reliable access platform.

Cisco Meraki MS Cloud -Managed Access Switches

- Virtually stack switches to monitor and configure thousands of switch ports instantly over the web
- Integrated Layer 7 analysis delivers network-wide visibility into users, devices, and applications
- Provision sites and remotely troubleshoot networks without onsite IT
- Integrated tools such as Power over Ethernet (PoE), PoE Plus, QoS, Link Layer Discovery Protocol (LLDP), and more ease voice and video deployments.

2366p011/a

Learn More

Compare Models

Cisco Cloud-Management

- Centrally manage campus and multi-site networks
- Integrated network-wide visibility and control
- Zero-touch device provisioning
- Seamless firmware updates and remote troubleshooting tools.

2366p012/a

Learn More

5.2.8.6 Software Defined Networks (SDN) — Controllers - is an application in software-defined networking (SDN) that manages flow control to enable intelligent networking. SDN controllers are based on protocols, such as OpenFlow, that

allow servers to tell switches where to send packets. The SDN controller lies between network devices at one end and applications at the other end. Any communications between applications and devices have to go through the controller. The controller uses multiple routing protocols including OpenFlow to configure network devices and choose the optimal network path for application traffic.

Cisco Response:

Cisco Extensible Network Controller

With its modular architecture and extensible protocol support, Cisco XNC offers exceptional extensibility. Built on top of the OpenDaylight controller, Cisco XNC is a platform for a number of useful and interesting applications. For example, Cisco will offer applications that perform campus slicing, networking monitoring, and custom routing capabilities. As with Cisco onePK, Cisco expects both commercial ISVs and the open source community to also develop applications on top of Cisco XNC.

Learn how Cisco Monitor Manager and Cisco eXtensible Network Controller (XNC) can provide greater business agility, through a cost-effective, scalable, Software-Defined Network (SDN)-based approach to traffic monitoring at: XNC.

5.2.8.7 Carrier Aggregation Switches — Carrier aggregation switches route traffic in addition to bridging (transmitted) Layer 2/Ethernet traffic. Carrier aggregation switches' major characteristics are:

- Designed for Metro Ethernet networks
- Designed for video and other high bandwidth applications
- Supports a variety of interface types, especially those commonly used by Service Providers

Capabilities should include:

- Redundant Processors
- Redundant Power
- IPv4 and IPv6 unicast and multicast
- High bandwidth
- Low latency
- Hot swappable power supplies and fans
- MPLS (Multiprotocol Label Switching)
- BGP (Border Gateway Protocol)
- Software router virtualization and/or multiple routing tables
- Policy based routing
- Layer 2 functionality
  - iv. Per VLAN Spanning Tree
  - v. Rapid Spanning Tree
  - vi. VLAN IDs up to 4096
  - vii. Layer 2 Class of Service (IEEE 802.1p)
  - viii. Link Aggregation Control Protocol (LACP)
  - ix. QinQ (IEEE 802.1ad)

Cisco Response:

Cisco Carrier Ethernet switches provide the aggregation and multiplexing layer between access and edge layers. Descriptions, benefits, and links to the detailed description of the carrier Ethernet switches included in the offering for this category are listed below.

ASR 9000 Series Aggregation Services Routers

- Offers nonstop video, enhanced scalability, and reduced carbon footprint
- Ideal for carriers offering residential, mobile and business services
- Scales up to 96 tbps per system with comprehensive system redundancy
- Offers unique service- and application-level intelligence.

Learn More

Data Sheets

Cisco 7600 Series Routers

- High performance, with up a choice of form factors purpose-built for high availability
- A portfolio of Shared Port Adapters (SPAs) and SPA Interface Processors (SIPs) that controls voice, video, and data experiences
- Scalable and extensible suite of hardware and software capabilities to enable intelligent Carrier Ethernet services
- Ideal for large enterprises and service providers.

Learn More

Data Sheets

ASR 903 Series Aggregation Router

- Provides high-performance, carrier-class access and pre-aggregation services
- Ideal for service providers that deliver carrier Ethernet or mobile backhaul services
- Offers fully redundant capabilities in a hardened small-form-factor chassis
- Protects investments with its modular and upgradable design.

Learn More

Data Sheets

Cisco Catalyst 6500 Series Switches

- Leading modular campus platform that simplifies operations, reduces costs, and optimizes existing investments
- Ideal for campus core and distribution, and for data center customers looking to deploy integrated service modules
- High availability with Virtual Switching System
- Integrated service modules for lower total cost of ownership and easy manageability.

Learn More

Data Sheets

Cisco Catalyst 4500E Series Switches

2366p014/a

- Highly expandable modular access and price/performance distribution switch
- Ideal for service providers, enterprises, and medium sized businesses
- Application visibility and control with Flexible NetFlow
- High availability with In Service Software Upgrade.

Learn More

Data Sheets

Compare Models

Cisco ME 4900 Series Switches

2366p015/a

- Addresses next-generation residential services
- High-performance, 1 rack-unit Carrier Ethernet switch
- Ideal for service providers that want to deploy new residential services
- Offers triple play service support (voice, video, and data)
- Industry-leading wire-speed performance of 48 Gbps and 71 mpps.

Learn More

Data Sheets

5.2.8.8 **Carrier Ethernet Access Switches** — A carrier Ethernet access switch can connect directly to the customer or be utilized as a network interface on the service side to provide layer 2 services.

- Hot-swappable and field-replaceable integrated power supply and fan tray
- AC or DC power supply with DC input ranging from 18V to 32 VDC and 36V to 72 VDC
- Ethernet and console port for manageability
- SD flash card slot for additional external storage
- Stratum 3 network clock
- Line-rate performance with a minimum of 62-million packets per second (MPPS) forwarding rate
- Support for dying gasp on loss of power
- Support for a variety of small form factor pluggable transceiver (SFP and SFP+) with support for Device Object Model (DOM)
- Timing services for a converged access network to support mobile solutions, including Radio Access Network (RAN) applications
- Support for Synchronous Ethernet (SyncE) services
- Supports Hierarchical Quality of Service (H-QoS) to provide granular traffic-shaping policies
- Supports Resilient Ethernet Protocol REP/G.8032 for rapid layer-two convergence

Cisco Response:

Implement class-leading switches featuring application intelligence, unified services, nonstop communications, virtualization, integrated security, and simplified manageability. Descriptions, benefits, and links to the detailed description of the Carrier Ethernet Access switches included in the offering for this category are listed below.

Cisco ME 2600X Series Switches

- Provide high service availability
- Offer flexible and differentiated services
- Manage and troubleshoot services remotely
- Improve security of network services to protect against malicious users.

Learn More

Data Sheets

Compare Models

Cisco ME 3600X Series Switches

2366p016/a

1 rack-unit, fixed switch that converges wireless and wireline services.

Ideal for service providers that want to simplify operations and deploy "pay-as-you-grow" business model.

Delivers premium services with hierarchical quality of service.

Provides 10 Gbps transport speed for business and mobile applications.

Learn More

Data Sheets

Compare Models

Cisco ME 3400E Series Switches

2366p018/a

- Customer-located Ethernet access switch optimized for business services
- Ideal for service providers that want to offer advanced Ethernet services such as Ethernet-to-the-Business VPN Services
- Offers platform for flexible and differentiated services
- Provides tools to deliver high service availability.

Learn More

Data Sheets

Compare Models

5.2.9 WIRELESS — Provides connectivity to wireless devices within a limited geographic area. System capabilities should include:

- Redundancy and automatic failover
- IPv6 compatibility
- NTP Support

5.2.9.1 **Access Points** — A wireless Access Point (AP) is a device that allows wireless devices to connect to a wired network using Wi-Fi, or related standards. Capabilities should include:

- 802.11a/b/g/n
- 802.11n
- 802.11ac
- Capable of controller discovery method via DHCP (onsite controller or offsite through Cloud Architecture)
- UL2043 plenum rated for safe mounting in a variety of indoor environments
- Support AES-CCMP (128-bit)
- Provides real-time wireless intrusion monitoring and detection

Cisco Response:

Cisco Aironet Series access points can be deployed in a distributed or centralized network for a branch office, campus, or large enterprise. To help ensure an exceptional end-user experience on the wireless network, these access points provide a variety of capabilities, including:

- Cisco Cleanair Technology, for a self-healing, self-optimizing network that avoids RF interference
- Cisco Clientlink 2.0 to improve reliability and coverage for existing clients
- Cisco Bandselect to improve 5 GHz client connections in mixed client environments
- Cisco Videostream, which uses multicast to improve multimedia applications.

Whether you need entry-level wireless for a small enterprise or mission-critical coverage at thousands of locations, the extensive Cisco Aironet Series product portfolio can provide the correct high-performance access point to meet your enterprise-class requirements.

Descriptions, benefits, and links to the detailed description of the Wireless Access Points included in the offering for this category are listed below:

- Cisco Aironet 3600 Series
- Cisco Aironet 3500 Series
- Cisco Aironet 2600 Series
- Cisco Aironet 1600 Series
- Cisco Aironet 700 Series.

5.2.9.2 **Outdoor Wireless Access Points** — Outdoor APs are rugged, with a metal cover and a DIN rail or other type of mount. During operations they can tolerate a wide temperature range, high humidity and exposure to water, dust, and oil. Capabilities should include:

- Flexible Deployment Options
- Provides real-time wireless intrusion monitoring and detection
- Capable of controller discovery method via DHCP (onsite controller or offsite through Cloud Architecture)

Cisco Response:

Cisco Aironet Outdoor access points can be deployed in a variety of demanding environments. To help ensure an exceptional user experience on the wireless network, these access points provide a variety of capabilities, including:

- Cisco CleanAir Technology for a self-healing, self-optimizing network that avoids RF interference
- Cisco ClientLink 2.0 to improve reliability and coverage for existing clients
- Cisco BandSelect to improve 5 GHz client connections in mixed client environments
- Cisco VideoStream, which uses multicast to improve multimedia applications.

Whether you need a multilevel mesh network, flexible options such as fiber-based backhaul, or even deployment in hazardous locations, the extensive Cisco Aironet 1550 Series product portfolio can provide a high-performance access point to meet your rugged outdoor requirements.

Descriptions, benefits, and links to the detailed description of the Outdoor Wireless Access Points included in the offering for this category are listed below:

- Cisco Aironet 1550 Series
- Cisco Aironet 1520 Series.

5.2.9.3 **Wireless LAN Controllers** — An onsite or offsite solution utilized to manage light-weight access points in large quantities by the network administrator or network operations center. The WLAN controller automatically handles the configuration of wireless access-points. Capabilities should include:

- Ability to monitor and mitigate RF interference/self-heal
- Support seamless roaming from AP to AP without requiring re-authentication
- Support configurable access control lists to filter traffic and denying wireless peer to peer traffic
- System encrypts all management layer traffic and passes it through a secure tunnel
- Policy management of users and devices provides ability to de-authorize or deny devices without denying the credentials of the user, nor disrupting other AP traffic
- Support configurable access control lists to filter traffic and denying wireless peer to peer traffic

Cisco Response:

Support small or large wireless network deployments with flexible deployment models, including new virtualization options. Descriptions, benefits, and links to the detailed description of the Wireless LAN Controllers included in the offering for this category are listed below.

8500 Series Wireless Controller

- High scalability in a single rack-unit space with centralized touch-point
- Management of up to 6000 Access Points, 64,000 clients, and 6,000 branch locations
- High speed with 10 GE connectivity support: 2 x 10 GE ports for redundancy
- Availability with sub-second access point and client stateful fail-over
- High resiliency with redundant dual power supplies.

Learn More

Data Sheet

Compare Products

Cisco 5760 Wireless LAN Controller

2366p020/a

- Wire-speed 60 Gbps throughput with advanced network services per controller
- Support for up to 1000 access points per controller and up to 12,000 clients per controller
- Scalability with seamless roaming across 72,000 access points
- High resiliency with N+1 clustering, link aggregation groups, and redundant power supplies
- Cisco IOS with features such as Flexible NetFlow, advanced QoS, and downloadable ACLs.

Learn More

Data Sheet

Compare Products

5500 Series Wireless LAN Controller

2366p021/a

- Use in enterprise campus deployments
- Allows connection of up to 500 access points
- Supports mobility services such as Cisco ClientLink and CleanAir technology
- Availability with sub-second access point and client stateful fail-over.

Learn More

Data Sheets

Compare Products

Cisco Catalyst 3850 Series Switches

- Best-in-class and feature-rich access platform with 480 Gbps stacking for gigabit desktop and 802.11ac wireless
- Converged wired and wireless access by extending wired features, resiliency, granular QoS, and scalability to wireless
- Distributed services across wired and wireless for security, policy, application visibility and control, and more
- Foundation for Cisco Open Network Environment enabled by a new ASIC with programmability and investment protection.

Learn More

Data Sheets

5.2.9.4 Wireless LAN Network Services and Management — Enables network administrators to quickly plan, configure and deploy a wireless network, as well as provide additional WLAN services. Some examples include wireless security, asset tracking, and location services. Capabilities should include:

- Provide for redundancy and automatic failover
- Historical trend and real time performance reporting is supported
- Management access to wireless network components is secured
- SNMPv3 enabled

- RFC 1213 compliant
- Automatically discover wireless network components
- Capability to alert for outages and utilization threshold exceptions
- Capability to support Apple's Bonjour Protocol / mDNS
- QoS / Application identification capability

Cisco Response:

Monitor access points, WLAN controllers, and more with services that offer scalable multi-device and multi-network application delivery. Descriptions, benefits, and links to the detailed description of the Wireless LAN Network Services and Management included in the offering for this category are listed below.

Cisco Prime Infrastructure

- Converged management for full lifecycle management of wired and wireless networks
- Improved configuration, change, and compliance management for lower TCO
- Integrated application assurance.

Learn More

Data Sheets

Mobility Services Engine

2366p022/a

- Enhance the performance of Cisco CleanAir
- Support improved wireless security with adaptive wireless intrusion protection services
- Detect presence and track and trace rogue devices, interferers, Wi-Fi clients, smart phones, and RFID tags with location services.

Learn More

Data Sheets

Advanced Location Services

- Location Analytics capture and analyze indoor location and historical trends to support greater visibility into customer movements and patterns
- Mobile Concierge helps engage users by delivering real-time context to their smart phones
- Mobile Concierge software developer's kit offers an easy-to-use approach for developing mobile applications and services for the Mobility Services Engine and providing highly personalized content.

Learn More

Data Sheet

5.2.9.5 Cloud-based services for Access Points — Cloud-based management of campus-wide WiFi deployments and distributed multi-site networks. Capabilities include:

- Zero-touch access point provisioning
- Network-wide visibility and control
- RF optimization,
- Firmware updates

Cisco Response:

Cisco Meraki Cloud Managed Wireless - Centrally manage campus and distributed wireless networks via the cloud. Descriptions, benefits, and links to the detailed description of the Cloud-based services for Access Points included in the offering for this category are listed below.

Cisco Meraki Cloud Managed Indoor Access Points

- 802.11n indoor and outdoor access points ranging from value-priced to high-performance models for high-density environments
- Enterprise-grade security with guest access and BYOD support built in
- Integrated application traffic shaping to prioritize critical apps and throttles, or to block unwanted apps
- Built-in wireless intrusion detection and protection services, mesh routing, Power over Ethernet support, and more.

Learn More

Compare Products

Cisco Meraki Cloud-Managed Outdoor Access Points

2366p023/a

- 802.11n outdoor access points designed for harsh, rugged, and outdoor environments (IP-67 rated)
- Enterprise-grade security with guest access and BYOD support built-in
- Integrated application traffic shaping prioritizes critical apps, throttles or blocks unwanted apps
- Built-in WIDS/WIPS, mesh routing, PoE support, and more
- Compatible with N-type external antennas.

Learn More

Compare Products

Cisco Meraki Cloud-Management

2366p024/a

- Centrally manage campus and multi-site networks
- Integrated network-wide visibility and control
- Zero-touch device provisioning
- Seamless firmware updates and remote troubleshooting tools.

Learn More

5.2.9.6 Bring Your Own Device (BYOD) — Mobile Data Management (MDM) technology utilized to allow employees to bring personally owned mobile devices (laptops, tablets, and smart phones) to their workplace, and use those devices to access privileged government information and applications in a secure manner. Capabilities should include:

- Ability to apply corporate policy to new devices accessing the network resources, whether wired or wireless
- Provide user and devices authentication to the network
- Provide secure remote access capability
- Support 802.1x
- Network optimization for performance, scalability, and user experience

Cisco Response:

Cisco provides a "one network, one policy, and one management" strategy for network access. This approach provides all the components you need to give your employees a consistently excellent experience across locations and devices.

Your IT staff can support greater mobility with high-performance, context-aware network solutions that go beyond BYOD. These solutions fully address a wide range of device, security, and business requirements.

Cisco and its partners can help your IT staff plan, build, and manage a BYOD Smart Solution that:

- Is comprehensive and highly secure
- Supports your business objectives
- Accelerates return on investment.

One Network

Cisco wired, Wi-Fi, and 3G and 4G networks are converging. Policy and management for wired and Wi-Fi networks are unified in a single solution. And Cisco virtualization experience infrastructure (Cisco VXI) offers policy-based access to desktops from anywhere, regardless of the underlying device or network. This consolidated approach provides a scalable platform for deploying new services.

Cisco VXI helps secure enterprise data in the data center, so you can take full advantage of evolving mobility and BYOD trends. The network is where the business policy is enforced through a combination of Cisco Identity Services Engine capabilities and network infrastructure (wireless or wired).

One Policy

To handle the surge of mobile devices on enterprise networks, your IT team must set policy centrally and automate enforcement. The Cisco Identity Services Engine replaces multiple, manually synchronized processes with a single point of policy across the organization. This single point of control helps IT create centralized policy that governs access to the network, whether wired or wireless.

Cisco ISE Product Highlights include:

- Consistent enforcement of context-based policies across wired and wireless networks
- System-wide visibility showing IT who and what is on the network's wired, wireless, or VPN
- Integrated AAA, profiling, posture, and guest services to simplify deployments and cut costs
- Device identification using ISE-based probes, embedded device sensors, endpoint scanning, and device feed service

- Greater visibility and control of the endpoint with Mobile Device Management solution integration
- Simplified BYOD onboarding through self-service registration.

Cisco ISE offers the following benefits:

- **Highly secure access** — Combine rigorous identification and enforcement with automated user onboarding for consistent access, control, and compliance
- **Greater worker productivity** — Get consistent and dependable access to services from anywhere and anytime
- **Lower operations costs** — Increase IT staff productivity by automating labor-intensive tasks and simplifying service delivery.

One Management

To support these ever-increasing mobile devices on the network, IT managers need solutions that give a single entry point for solving access and experience problems. Cisco Prime Infrastructure management solutions provide a single workflow to identify problems by user, rather than by network element.

Experience monitoring, fed with network instrumentation and intelligence, provides a single source of truth for application performance.

Listed below are the products offered in this category as well as links to the detailed descriptions.

Security

- Cisco Identity Services Engine
- Cisco AnyConnect
- Cisco BYOD Smart Solution At-A-Glance (pdf - 445 KB)
- Cisco Trustsec At-A-Glance (pdf - 598 KB)
- Cisco Identity Services Engine At-A-Glance (pdf - 839 KB)
- Cisco AnyConnect Secure Mobility Solution At-A-Glance (pdf - 166 KB)
- Cisco ASA 5500 Series Adaptive Security Appliances At-A-Glance (pdf - 677 KB)
- Cisco ASA 5500 Series IPS Solution At-A-Glance (pdf - 276 KB)
- Highly Secure Mobility With Cisco Scansafe (Data Sheet) (pdf - 377 KB)
- Cisco Any Device: Planning a Productive and Highly Secure Future (White Paper) (pdf - 1.2 Mb)
- The Future of Network Security: Cisco SecureX (White Paper).

Infrastructure

- Cisco Aironet 3600 Series Access Points
- Cisco Wireless LAN Controllers
- Cisco Prime Infrastructure
- Cisco Prime Assurance.

Collaboration

- Cisco Jabber
- Cisco WebEx Technology.

Cisco Services

- Cisco Services for BYOD and the Unified Workspace (pdf - 499 KB).

5.3.0 UNIFIED COMMUNICATIONS (UC) — A set of products that provides a consistent unified user interface and user experience across multiple devices and media types. Unified Communications that is able to provide services such as session management, voice, video, messaging, mobility, and web conferencing. It can provide the foundation for advanced unified communications capabilities of IM and presence-based services and extends telephony features and capabilities to packet telephony network devices such as IP phones, media processing devices, Voice over IP (VoIP) gateways, and multimedia applications. Additional services, such as unified messaging, multimedia conferencing, collaborative contact centers, and interactive multimedia response systems, are made possible through open telephony APIs. General UC solution capabilities should include:

- High Availability for Call Processing
- Hardware Platform High Availability
- Network Connectivity High Availability
- Call Processing Redundancy

Cisco Response:

Extend Communications

Provide reliable and advanced communications capabilities for your staff no matter where they are working, with a full suite of IP Communications solutions and endpoints. Manage voice, video, mobility, and presence services between IP endpoints, media-processing devices, Voice-over-IP (VoIP) gateways, mobile devices, and multimedia applications.

Cisco IP Communications products can also help your business:

- Efficiently run voice, data, and video communications over a single, converged network
- Take advantage of a wide array of Cisco IP endpoints to meet diverse communications needs
- Optimize efficiency with Cisco Unified Communications network management.

A list of the products offered for this category, and links to the detailed description of the Unified Communications solutions included in the offering for this category are listed below.

Cisco Unified Communications Platform

Cisco Unified Communications Applications

- Cisco Paging Server
- Cisco Unified Attendant Consoles
- Cisco Unified Communications Manager
- Cisco Unified Communications Manager Express
- Cisco Unified Communications Manager Session Management Edition.

Cisco Business Edition

- Cisco Business Edition 3000
- Cisco Business Edition 6000.

Cisco Unified Communications Infrastructure

- Cisco Intercompany Media Engine (IME)
- Cisco Unified Communications On the Cisco Unified Computing System
- Cisco Unified Border Element (CUBE)
- Cisco Unified Survivable Remote Site Telephony (SRST)
- Cisco Media Convergence Servers (MCS)
- Cisco Prime Collaboration.

Cisco Unified Communications Gateways

- Cisco Unified Communications Gateways
- Cisco Voice and Video Conferencing For Cisco Integrated Service Routers (ISR)
- Cisco Digital Gateway
- Cisco VG200 Series Gateways
- Cisco Small Business Voice Gateways and ATAS.

Cisco Unified Messaging

- Cisco Unity Connection
- Cisco Unity Express.

Cisco Unified Communications Endpoints

- Accessories.

Cisco Unified IP Phones

- Cisco Unified SIP Phones 3900 Series
- Cisco Unified IP Phones 6900 Series
- Cisco Unified IP Phones 7900 Series
- Cisco Unified IP Phones 8800 Series
- Cisco Unified IP Phones 8900 Series
- Cisco Unified IP Phones 9900 Series
- Cisco Desktop Collaboration Experience DX600 Series
- cisco Unified Video Advantage (CUVA)
- Cisco Jabber
- Cisco Webex Connect Client
- Cisco Midsize Business Solutions

Cisco Unified Communications Virtualization

- Cisco Collaboration Solutions (HCS)
- Cisco Unified Communications ON UCS

Cisco Unified Communications Licensing and Subscription

- Cisco Hosted Collaboration Solutions (HCS)
- Cisco Unified Workspace Licensing (CUWL)
- Cisco Unified Communications Software Subscription (UCSS)

5.3.0.1 **IP Telephony** — Solutions utilized to provide the delivery of the telephony application (for example, call setup and teardown, and telephony features) over IP, instead of using circuit-switched or other modalities. Capabilities should include:

- Support for analog, digital, and IP endpoints
- Centralized Management
- Provide basic hunt group and call queuing capabilities

- Flexibility to configure queue depth and hold time, play unique announcements and Music on Hold (MoH), log in and log out users from a queue and basic queue statistics (from the phone
- E911 Support

Cisco Response:

Secure, Reliable Voice Calls over Your Network

IP telephony transmits voice communications over the network using open, standards-based Internet Protocol.

It provides a way for you to extend consistent voice communications services to all your employees in their workspaces -- on the main campus, at branch offices, remote, or mobile.

Cisco IP telephony solutions are an integral part of Cisco Unified Communications, which unify voice, video, data, and mobile applications on fixed and mobile networks. Your employees can talk with each other using almost any media, device, or operating system.

Using your network as the platform, your organization can gain the inherent benefits of a converged network for transport and interconnection. IP telephony makes it easier to:

- Provide highly secure, reliable, scalable communications that take advantage of your LAN and WAN
- Improve employee flexibility and productivity with the full range of Cisco Unified Communications and third-party applications
- Take advantage of a wide range of Session Initiation Protocol (SIP)-based capabilities.

Deliver consistent communication services to all of your employees in their workspaces with this full suite of solutions and endpoints included in this offering. A description of the products or solutions offered click on the links below.

Cisco Unified Communications Gateway Services

- Cisco TDM Gateways
- Analog Gateway
- Cisco Unified Survivable Remote Site Telephony
- Cisco Unified Border Element
- Cisco Unified Communications Manager Express
- Cisco Unity Express
- Video Conferencing Solutions
- Mobility Workforce Architecture
- Cisco Unified SIP Proxy.

Cisco Integrated Services Routers (ISR)

- Cisco 3900 Series Integrated Services Routers
- Cisco 2900 Series Integrated Routers
- Cisco 1861e Series Integrated Services Router
- Cisco 881 Integrated Services Router
- Cisco 887v Integrated Services Router
- Cisco 888e Integrated Services Router
- Cisco 888 Integrated Services Router.

Cisco ASR 1000 Series Aggregation Services Routers

- Cisco ASR 1006 Router
- Cisco ASR 1004 Router
- Cisco ASR 1001 Router.

Cisco VG200 Series Gateways

- Cisco VG224 Analog Voice Gateway
- Cisco VG204 Analog Voice Gateway
- Cisco VG202 Analog Voice Gateway.

Cisco AS5400 Series Universal Gateways

- Cisco AS5400XM Universal Gateway.

Other Services and Solutions

- Cisco UCS Express
- Cisco Service Advertisement Framework (SAF)
- Cisco Enterprise Medianet
- Cisco AS5350XM Universal Gateway
- Cisco RSVP Agent
- Cisco UC Gateway Services API.

5.3.0.2 Instant messaging/ Presence — Solutions that allow communication over the Internet that offers quick transmission of text-based messages from sender to receiver. In push mode between two or more people using personal computers or other devices, along with shared clients, instant messaging basically offers real-time direct written language-based online chat. Instant messaging may also provide video calling, file sharing, PC-to-PC voice calling and PC-to-regular-phone calling.

Cisco Response:

Streamline communications and enhance productivity with Cisco Enterprise Instant Messaging. Listed below are the products included in this category offering as well as links to the detailed descriptions.

- Cisco WebEx Connect
- Jabber.

5.3.0.3 Unified messaging — Integration of different electronic messaging and communications media (e-mail, SMS, Fax, voicemail, video messaging, etc.) technologies into a single interface, accessible from a variety of different devices.

- Ability to access and manage voice messages in a variety of ways, using email inbox, Web browser, desktop client, VoIP phone, or mobile phone
- Visual Voicemail Support (Optional)

Cisco Response:

With Cisco voice and unified messaging solutions, you can take control of your communications experience. Cisco has a messaging solution for you, whether you need:

- Basic voicemail
- Integrated messaging with email, web, and mobile clients
- Unified messaging with all voice, fax, and email messages stored in the same inbox.

These solutions offer industry-leading features that can improve your productivity. For example, you can manage your voice messages when you want from your preferred device - computer, tablet, smartphone, desk phone, and more.

Flexibility, Reliability, and Security

Cisco voice and unified messaging solutions integrate with traditional call control and voicemail systems, and the latest unified communications applications. These flexible deployment options provide cost savings, excellent reliability, and support highly secure messaging to protect your privacy.

Find Your Solution

The Cisco voice and unified messaging portfolio has a solution for organizations of all types and sizes. Listed below are the products included in this category offering as well as links to the detailed descriptions.

- Cisco Unity Connection: Voicemail or unified messaging with speech recognition on an easy-to-manage platform for organizations of all sizes
- Cisco Unity Express: Cost-effective integrated voice messaging, auto attendant, and Interactive Voice Response (IVR) on a Cisco Integrated Services Router for enterprise branches and small offices
- Cisco Unified Survivable Remote Site Voicemail: Communications protection with voicemail survivability for your organization's remote sites, such as branch offices or other small sites.

5.3.0.4 Contact Center — A computer-based system that provides call and contact routing for high-volume telephony transactions, with specialist answering "agent" stations and a sophisticated real-time contact management system. The definition includes all contact center systems that provide inbound contact handling capabilities and automatic contact distribution, combined with a high degree of sophistication in terms of dynamic contact traffic management.

Cisco Response:

Cisco Unified Contact Center delivers intelligent contact routing, call treatment, network-to-desktop Computer Telephony Integration (CTI), and multichannel contact management over an IP infrastructure. It combines multichannel Automatic Call Distributor (ACD) functionality with IP telephony in a unified solution, enabling your company to rapidly deploy a distributed contact center infrastructure.

Gartner Names Cisco a Leader:

Cisco named a leader in the 2012 Gartner Magic Quadrant for Contact Center Infrastructure, Worldwide.

Cisco Unified Contact Center Enterprise provides:

- Segmentation of customers, and monitoring of resource availability
- Delivery of each contact to the most appropriate resource anywhere in the enterprise
- Comprehensive customer profiles using contact-related data, such as dialed number, and calling line ID
- Routing to the most appropriate resource to meet customer needs based on real-time conditions (such as agent skills, availability, and queue lengths)
- Presence integration to increase caller satisfaction through improved agent performance, and knowledge-worker expertise.

Listed below are the products included in this category offering as well as links to the detailed descriptions.

Cisco Unified Contact Center Enterprise

- Deliver state-of-the-art contact center capabilities for enterprise applications
- Support both premise-based and hosted deployments with Cisco Unified Communications Manager or third-party ACDs
- Provide intelligent contact routing, call treatment, network-to-desktop CTI, and multichannel contact management
- Take advantage of desktop options such as a web-based thin client collaborative desktop for agents and supervisors.

Learn More

Data Sheets

Cisco Unified Contact Center Express

- Easily deploy and use highly secure, virtual, and highly available sophisticated call routing and contact management capabilities for your contact center
- Ideal for midmarket, enterprise branch, or corporate departments
- Ideal for both formal and informal contact centers
- Take advantage of support for Web 2.0 agent desktop SDK for custom desktop development.

Learn More

Data Sheets

Cisco Unified Customer Voice Portal

- Provide speech-enabled self-service to callers with this award-winning product
- Allow calls to be treated at the most efficient location with powerful call control
- Combine open standards support for speech recognition with intelligent application development
- Deliver personalized self-service as a standalone IVR system, or integrate transparently with the contact center.

Learn More

Data Sheets

Cisco SocialMiner

- Provides a social media campaign management solution
- Monitors the social web for relevant public customer postings and helps you engage with customers proactively
- Offers context about customers by providing a social screen pop to customer service agents or other responders
- Helps you manage your brand by monitoring and responding to social media posts from customers who need assistance.

Learn More

Data Sheets

5.3.0.5 Communications End Points and Applications

- Attendant Consoles
- IP Phones

Cisco Response:

Cisco Unified Communications Endpoints

- Accessories.

Cisco Unified IP Phones

- Cisco Unified SIP Phones 3900 Series
- Cisco Unified IP Phones 6900 Series
- Cisco Unified IP Phones 7900 Series
- Cisco Unified IP Phones 8800 Series
- Cisco Unified IP Phones 8900 Series
- Cisco Unified IP Phones 9900 Series
- Cisco Desktop Collaboration Experience DX600 Series
- Cisco Jabber
- Cisco Webex Connect Client
- Cisco Midsize Business Solutions.

Virtualized Endpoints

- Cisco Virtualization Experience Client 6000 Series
- Cisco Virtualization Experience Client 4000 Series
- Cisco Virtualization Experience Client 2000 Series
- Cisco Virtualization Experience Client Manager
- Cisco Virtualization Experience Media Engine.

5.3.0.6 UC Network Management — Provides end-to-end service management for Unified Communications. Capabilities include testing, performance monitoring, configuration management, and business intelligence reporting.

Cisco Response:

Cisco Unified Communications is a comprehensive portfolio of applications integrated with a highly secure network infrastructure.

These network management applications are tailored and optimized to provide complete provisioning, operations, monitoring, and reporting.

Large Enterprises

The Cisco Prime Unified Communications Management suite helps to increase operational efficiency for enterprises with 500 to 30,000 devices. It offers an integrated set of products with a single view into the entire Cisco Unified Communications solution.

Feature and Capabilities

Cisco Prime Collaboration helps enable rapid installation and maintenance of Cisco Unified Communications components as well as the provisioning of users and services, substantially increasing productivity and lowering operating expenses. By significantly reducing the complexity in performing

moves, adds, and changes, the solution facilitates delegation of these tasks. This helps network operators to optimize IT resources and further reduce total cost of ownership.

This solution also provides efficient, integrated assurance management of applications and the underlying transport infrastructure. This includes real-time monitoring and troubleshooting of Cisco TelePresence solutions and the entire Cisco Unified Communications system. The solution expedites operator resolution of service quality issues before they affect end users and helps avoid system and service outages for a greater end user quality of experience.

Cisco Prime Collaboration also provides historical reporting of key performance indicators and enables IT network managers to analyze trends for capacity planning, resource optimization, and quality of service. The solution helps track collaboration technology adoption rates in the network and provides metrics to help analyze how users are actually using the collaboration endpoints daily. It also can show status and rollout progress of a collaboration network deployment.

Cisco Prime Collaboration offers:

- Efficient, policy-based provisioning of Cisco Unified Communications users and services through a single interface
- Delegation of voice provisioning changes for operational savings
- Real-time monitoring of voice and video networks with dashboard summaries and alarm correlation
- Consistent, reliable service delivery through proactive fault detection and rapid isolation
- Advanced diagnostics tools, including traffic simulation and testing of circuits and endpoints to help identify core issues
- Trend analysis and reporting to simplify long-term planning and facilitate deployment analysis.

See the many benefits of Cisco Unified Communications Management suite.

The entire product portfolio can be found at: Cisco Prime Collaboration.

5.3.0.7 Collaboration — Voice, video, and web conferencing; messaging; mobile applications; and enterprise social software.

Cisco Response:

Collaboration is more than a technical architecture, solution, or product; it is the experience that integrates people, processes, and technology. We believe that by working together, people can achieve extraordinary things.

An org chart may show hierarchy, but it doesn't represent how people actually interact inside, outside, and across the organization. Finding ways to improve the connections between people and the information they need to share is at the center of improving business productivity.

Empower, Engage, Innovate

The goal - and the power - of collaboration technology is to fulfill the human affinity to share as naturally as possible. How do you get there?

- Empower people to work their way - where, when, and how they want - without limits
- Engage people by providing the best collaboration tools to connect with peers and other organizations
- Allow people to innovate and become more creative in developing ideas and solving problems.

People don't want to have to think about "how do I?" just about "what do I want to do?" The key is to implement intuitive technologies that let people focus on meeting business goals, shifting the focus from individual applications to integrated collaboration experiences.

The New Collaborative Environment

Opportunity comes from the combination of technology and people. The collaborative workspace environment gives people the flexibility to be where they need to be to do the best work they can.

Cisco uses an architecture-based approach, integrating the mobile, social, visual, and virtual aspects of collaboration to bring people together anytime, anywhere, on any device. Connect employees, customers, and suppliers to make decisions, resolve customer issues, or address supply-chain challenges. The architecture cost effectively enables this with scale, security, and accessibility. The Cisco holistic collaboration strategy and architecture account not only for the technology, but what it means to your processes and culture.

Implementing collaboration solutions allows you to:

- Flatten organizational hierarchy and better communicate with all levels of the organization
- Elevate and personalize communications to improve the quality and speed of decisions
- Save time, simplify workflows, and increase workforce interaction and productivity
- Build trust and understanding across time zones within cross-functional teams through frequent video communications
- Improve customer responsiveness by facilitating faster access to experts and information
- Reduce travel, real-estate costs, and greenhouse gas emissions by meeting virtually and supporting telecommuting.

Listed below are the products included in this category offering as well as links to the detailed descriptions.

All Collaboration Applications

Stay connected and productive with voice, video, and web conferencing; messaging; mobile applications; and enterprise social software solutions included in this offering. Collaboration solutions include:

Cisco Webex Meetings

- Meet with anyone online to present, share, and collaborate
- Organize and manage all meeting activities, and easily share files
- Accelerate business results, increase team productivity, and lower costs
- Cisco also offers a full suite of Conferencing Applications.

Learn More

Datasheets

Product Comparison

Cisco Jabber

- New unified communications applications solution lets you collaborate from any workspace
- Easy access to presence, IM, voice and video, voice messages, desktop sharing, and conferencing
- Consistent experience across PC, MAC, IPHONE, IPAD, ANDROID, NOKIA, and BLACKBERRY devices.

2366p025/a

Learn More

Cisco WebEx Social

- Combines the power of enterprise social networking, content creation, and real-time communications
- Instantly share information and knowledge across teams, departments and geographies
- Enable employees anywhere to quickly find the people and resources they need to get work done
- Create and capture intellectual capital in one secure, centralized location.

Learn More

Data Sheets

5.3.0.8 Collaborative Video — A set of immersive video technologies that enable people to feel or appear as if they were present in a location that they are not physically in. Immersive video consists of a multiple codec video system, where each meeting attendee uses an immersive video room to "dial in" and can see/talk to every other member on a screen (or screens) as if they were in the same room and provides call control that enables intelligent video bandwidth management.

Cisco Response:

Use the Power of In-Person Collaboration

How do you promote bigger ideas and better innovation? Make it easy for your experts to put their heads together. Cisco TelePresence offers the easiest, most dynamic way for dispersed teams to get together. It's where talent and technology meet.

See Cisco Telepresence and Explore the Benefits For Yourself

Not only can you bring experts together to solve problems on the fly, but you can also use the power of TelePresence to unify your supply chain, provide highly engaged customer service, train remote teams, and more. Think beyond the boardroom. Transform your business processes with Cisco TelePresence.

Cisco TelePresence helps you:

- **Make the Best Use of Employee Time** — Frequent video participants report saving at least 2 hours weekly, with one-third reporting at least 1 day saved per week. Telepresence solutions have helped them save money, improve work-life balance, increase their competitive advantage, and bring people closer together.
- **Speed Decision Making** — Accelerate business-critical decision making, shorten sales cycles, reduce time to market, and create new forums for collaboration.
- **Cut Travel Costs** — Many customers reduce their business travel by 30 percent or more when implementing TelePresence. In fact, the cost of two international business trips will pay for a video conferencing system. Trygvesta, a large Nordic insurance company with 2 million customers, reduced travel from 180 to 130 trips per month, saving at least $120,000.
- **Consider the Opportunity Costs** — The true cost of travel is not just a plane ticket and hotel. Time on the road could be spent being more productive, bringing new products to market, reducing repair time, or meeting with more clients. Use the Business Advantage Calculator to see how video can benefit your business in particular.
- **Transform Business Processes** — TelePresence makes it easy for teams to collaborate, innovate, and resolve issues. Now you can bring those benefits to customer service, supply chain management, and training; redefine best practices; and accelerate ROI even more.
- **Be Greener** — Here is another way to reduce CO2 emissions: 100 employees using video once a week instead of commuting would save the equivalent of a forest the size of five football fields.

Listed below are the products included in this category offering as well as links to the detailed descriptions.

Cisco Pervasive Conferencing

- Simplify rich multiparty collaboration
- Deliver ubiquitous conferencing experiences on any device, anywhere
- Bring everyone together on mobile to immersive video systems
- Enhance efficiency and ROI from your conferencing infrastructure.

Learn More

Cisco Telepresence TX9000 Series

- New industrial design for greater immersion
- Three very high quality simultaneous video streams and a high-definition, full-motion content sharing stream for unparalleled video and content collaboration
- Superior lighting and sound, discreet camera housing, touch-screen interface
- Helps reduce TCO with 20 percent lower bandwidth requirements than earlier model, faster installation, and easy servicing.

Learn More

Data Sheets

Cisco Capture, Transform, Share

- Deliver an engaging viewing experience for your Video on Demand (VOD) or live streaming video content
- Convert video endpoints into a recording studio
- Transform and customize video content to be viewed on any device and environment
- Share content and empower users to search and navigate by spoken keywords or speakers.

Learn More

Cisco Telepresence SX20 Quick Set

- Easily turn a flat panel display into a sleek, powerful TelePresence system
- Multipoint support accommodates three additional callers
- Three camera choices and dual-screen option offer room size and configuration flexibility.

Learn More

Data Sheet

Cisco Telepresence Server 7010 and MSE 8710

- Compatible with all major vendors' endpoints for multipoint calls
- Facilitates multi-screen and multi-stream interoperability through TIP
- Supports Cisco ActivePresence to enhance the user experience
- Provides an exceptionally high-density, high-capacity video bridge
- Supports up to 720p resolution at 60 frames per second and 1080p resolution at 30 frames per second
- Available as a chassis-based platform or as an appliance.

Learn More

5.3.0.8.1 **Content Delivery Systems (CDS)** — A large distributed system of servers deployed in multiple data centers connected by the Internet. The purpose of the content delivery system is to serve content to end-users with high availability and high performance. CDSs serve content over the Internet, including web objects (text, graphics, URLs, and scripts), downloadable objects (media files, software, documents), applications (e-commerce, portals), live streaming media, on-demand streaming media, and social networks.

Cisco Response:

Deploy a media delivery system that improves the reach, quality, and user experience of video applications. The Cisco Enterprise Content Delivery System is a predictable, scalable, and versatile solution that helps organizations optimize video distribution over their existing WAN infrastructure. As a core component of the Cisco medianet architecture, the Cisco Enterprise Content Delivery System integrates into your existing network. When deployed with CISCO WIDE AREA APPLICATION SERVICES, it provides a complete WAN optimization solution for video.

Now it's easier for you to deploy video at scale for:

- Training and education
- Events
- Organizational communications.

Flexible Deployment Models Deliver Predictable Network Performance

The Cisco Enterprise Content Delivery System uses two network appliances and a virtual blade with versatile capabilities that can deliver streamed and on-demand video to end users on all types of video endpoints. This system can be scaled to support small sites with less than 25 users or large campuses with thousands of users. This versatile solution simultaneously supports media formats such as:

- Adobe Flash
- Windows Media
- Apple QuickTime
- H.264 video compression standards.

With the Cisco Enterprise Content Delivery System, you can take full advantage of video as a reliable tool to enhance productivity and increase the value of business communications.

Products and services included as part of this offering are described at the links below:

- Integrated Services Router Generation 2
- Digital Media Suite Introduction
- Wide Area Application Services Introduction.

5.3.0.8.2 **Physical Security** — Technology utilized to restricting physical access by unauthorized people to controlled facilities. Technologies include:

a. Access control systems
b. Detection/Identification systems, such as surveillance systems, closed circuit television cameras, or IP camera networks and the associated monitoring systems.
c. Response systems such as alert systems, desktop monitoring systems, radios, mobile phones, IP phones, and digital signage
d. Building and energy controls

Cisco Response:

Build cost-effective, modular, best-in-class physical security solutions that interoperate with your existing systems. Engineered with network and video expertise, Cisco Physical Security Solutions:

- Include video surveillance, access control, and incident response and notification
- Are easy to deploy, use, and maintain
- Integrate tightly with Cisco IP network (Medianet)
- Protect existing investments as you migrate
- Support open standards.

Using the network as an open, scalable platform for integrating security provides businesses with several benefits, such as operational flexibility, greater protection capabilities, lower cost of ownership, and reduced risk.

Cisco Physical Security products provide video surveillance, IP cameras, access control, and incident response solutions. Listed below are the products included in this category offering as well as links to the detailed descriptions.

- Connected Physical Security
- Interoperability Systems.

Connected Physical Security

IP Video Surveillance

- Cisco Physical Security Operations Manager
- Cisco Video Analytics
- Cisco Video Surveillance Encoding Server
- Cisco Video Surveillance Manager
- Cisco Video Surveillance Media Server Software
- Cisco Video Surveillance Operations Manager Software
- Cisco Video Surveillance Storage System
- Cisco Video Surveillance Virtual Matrix Software.

Physical Access Control

- Cisco Physical Access Gateways
- Cisco Physical Access Manager.

Physical Security Platforms

- Cisco Physical Security Multiservices Platform Series
- Virtualized Applications For UCS.

Video Surveillance IP Cameras

- Cisco Video Surveillance 7000 Series IP Cameras
- Cisco Video Surveillance 6000 Series IP Cameras
- Cisco Video Surveillance 4000 Series IP Cameras
- Cisco Video Surveillance 3000 Series IP Cameras
- Cisco Video Surveillance Encoders

- Cisco Video Surveillance IP Camera Accessories
- Cisco Video Surveillance PTZ IP Cameras.

Interoperability Systems

- Cisco IP Interoperability and Collaboration System
- Cisco IPICS Deployment Options
- Cisco IPICS Operational Views
- Cisco IPICS Phone Client
- Cisco IPICS PMC Client Software
- Cisco IPICS Policy Engine
- Cisco IPICS Server Software.

5.3.1 SERVICES — For each Category above (5.21-5.30), the following services should be available for procurement as well at the time of product purchase or anytime afterwards.

Cisco Response:

Cisco attempts to meet and exceed the expectations of our customers in terms of the maturity, professionalism, and effectiveness of our service delivery. We offer an array of service portfolios, customized to the special needs of different market segments and technologies. Our goal is to help customers of all types realize the full potential of their multi-service networks.

J.D. Power and Associates 2012 Certification

Recognized by J.D. Power and Associates for providing "An Outstanding Customer Service Experience." Cisco is the only company to have achieved CTSS certification six times.

The following distinctive achievements in service delivery and resources demonstrate Cisco's leadership:

- **Automated Support:** Cisco.com automates a wide variety of tools and processes, including a set of Internet commerce tools that allow customers to buy Cisco products and services online, and check the availability and status of spare parts. Cisco.com also automates the troubleshooting of many common support issues.
  - 79 percent of all customer technical support issues are solved online
  - Over 306,000 technical support issues resolved online each month
  - Over 2 million unique visitors per month
  - 3+ million software downloads per month.
- **Large Global Pool of Skilled Technicians:** Cisco offers our customers a large global team of proficient support engineers.
  - Over 1500 technical support professionals worldwide averaging of 5 to 10 years' experience in solutions
  - Over 500 Cisco Certified Internetworking Experts (CCIEs).
- **Global Support Infrastructure:** Cisco maintains a state-of-the-art global logistics infrastructure to meet the critical mission demands of our customers:
  - Over 900 parts depots with over 170,000 parts delivered every quarter
  - Geographic coverage in 120+ countries
  - Over $4 billion in parts inventory
  - Consistent refresh of parts inventory and software loads

- Access to globally deployed field engineers
- Hardware replacement options include 2 hour, 4 hour, and next business day.

- **Secure Supply Chain:** In recognition of growing awareness of the role that supply chain security plays in increasingly critical cyber security strategies, Cisco has a dedicated team within its supply chain organization to better address supply chain security threats and vulnerabilities. This team continually assesses, monitors, and improves Cisco supply chain security for the entire lifecycle of products, systems, and services, and so helps to ensure product integrity for our customers.
- **Expert Consulting Teams:** Cisco's Internet Business Solutions Group (IBSG) and Customer Success Engineering (CSE) team assess the business needs of service providers and pioneer the building of their next-generation networks, helping identify new sources of revenue and decrease operational expenses.
- **Network Availability:** Cisco Services like Operational Readiness Assessment and Network Reliability Improvement Analysis reflect the Cisco commitment to help you achieve redundancy and high network availability.
- **Evolving Services to Meet Your Needs**: Cisco provides industry-leading service capabilities and processes that are flexible enough to address your needs today and in the future. Your feedback, along with that of other customers, is acted upon through an evaluation process that promotes product, service, and process improvements. Cisco is committed to delivering an exceptional service experience that is flexible enough to meet your needs today and in the future.

5.3.1.1 Maintenance Services — Capability to provide technical support, flexible hardware coverage, and smart, proactive device diagnostics for hardware.

Cisco Response:

At Cisco maintenance services are referred to as Technical Services. Cisco Technical Services help you increase operational efficiency, lower support costs, and improve availability risk management through automated network-equipment inventory management and award-winning support. With these services, you can:

- More effectively manage risk, plan for equipment upgrades, and comply with your corporate policies
- Identify and resolve issues quickly and reduce downtime
- Streamline contract management and access support resources faster.

Product Support

Product Support Services help you increase operational efficiency, lower support costs, and improve availability risk management through automated network-equipment inventory management and award-winning support. With these services, you can:

- More effectively manage risk, plan for equipment upgrades, and comply with your corporate policies
- Identify and resolve issues quickly and reduce downtime
- Streamline contract management and access support resources faster.

Examples of Product Support Services for Enterprise include:

- SMARTnet Total Care
- SMARTnet Service
- Essential Operate Services
- Telepresence Essential Operate Services
- Cisco Services For Intrusion Prevention System (IPS)

- Cisco Smart Foundation
- Cisco Mission Critical Support Service
- Cisco Security Intellishield Alert Manager Service.

Solution Support Services help you increase solution uptime and employee productivity by providing priority access to dedicated and focused resources to manage, troubleshoot, and speed resolution of issues that might arise within complex, multivendor solutions. They supplement product-level technical support to:

- Quickly isolate and resolve issues that may arise within the solution
- Improve the performance of IT and network operations
- Increase the availability of the applications supported within the solution.

Examples of Solution Support Services:

- Cisco Solution Support Services (pdf - 280 KB).

Under the contract, Cisco is pleased to make available its full portfolio of maintenance and professional services. A full description of each service and service level can be viewed at the following site:

http://www.cisco.com/web/about/doing_business/legal/service_descriptions/index.html

5.3.1.2 Professional Services

- Deployment Services
  - Survey/ Design Services — Includes, but not limited to, discovery, design, architecture review/validation, and readiness assessment.
  - Implementation Services — Includes, but not limited to, basic installation and configuration or end-to-end integration and deployment.
  - Optimization — Includes, but not limited to, assessing operational environment readiness, identify ways to increase efficiencies throughout the network, and optimize Customer's infrastructure, applications and service management.
- Remote Management Services — Includes, but not limited to, continuous monitoring, incident management, problem management, change management, and utilization and performance reporting that may be on a subscription basis.
- Consulting/Advisory Services — Includes, but not limited to, assessing the availability, reliability, security and performance of Customer's existing solutions.
- Data Communications Architectural Design Services — Developing architectural strategies and roadmaps for transforming Customer's existing network architecture and operations management.
- Statement of Work (SOW) Services — Customer-specific tasks to be accomplished and/or services to be delivered based on Customer's business and technical requirements.

Cisco Response:

WSCA-NASPO members can leverage Cisco's entire portfolio of professional services. Regardless of the technology being deployed under the contract, Cisco's methodology for professional services provides a comprehensive approach to managing all aspects of your network and uses a three-phased approach – Plan, Build, and Manage. **Figure 10** depicts the key services available during each of the phases.

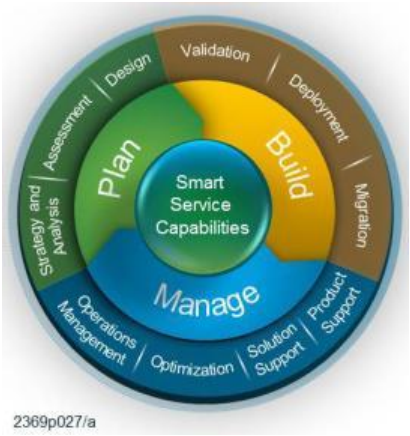

Figure 10. Cisco's Professional Services Model

Within each of these three phases, there are a variety of service offerings available to WSCA-NASPO customers. Below you will find a brief description of the services offered within our portfolio.

Plan: Develop an architectural strategy, transformational road map, and design.

Strategy and Analysis

Strategy and Analysis Services help you to effectively support new and future business requirements by creating architectural strategies and roadmaps for transforming your network architecture and operations management. They can help enable you to:

- Prioritize and focus architecture transformation and network operations and engineering management efforts
- Accelerate the development of a cost-effective strategy with a measurable ROI
- Successfully transform your infrastructure, management, people, and processes.

Assessment

Assessment Services help you determine your IT and network infrastructure's compliance to best practices and policies and/or readiness to support a new technology, application, architecture, or solution, to help you:

- Reduce deployment costs and adoption delays
- Improve your operations team's ability to support what is being introduced
- More effectively budget by accurately identifying incremental investment requirements.

Design

Design Services help you create a flexible, resilient, scalable architectural foundation to support your business solutions by developing designs for your IT and network infrastructure, applications, operations processes, and network management. They can help enable you to:

- Improve your network infrastructure performance, security, and scalability
- Accelerate adoption of new technologies and improve return on investment
- Reduce expensive and time-consuming redesign
- Strengthen the proficiency of your deployment team and operations team.

Build: Validate, implement, and migrate new solutions and applications.

Validation

Validation Services help you confirm that your solution meets your requirements for availability, security, reliability, and performance through assessment and issue resolution in a lab environment before implementation in your production network. This helps you to:

- Mitigate risks associated with updating the production network
- Accelerate time to market and solution adoption
- Reduce costly delays, risks, and rework
- Improve availability.

Deployment

Deployment Services help you successfully deploy new IT and network solutions or applications. Expert assistance helps you to:

- Reduce delays, rework, and other problems during implementation
- Decrease disruption to your production network during deployment
- Realize business and technical goals of the new solution.

Migration

Migration Services help you to control costs, improve operational excellence, and mitigate risk during device, network, and software refreshes. With a systematic, holistic, efficient approach to upgrading the network infrastructure, these will help you:

- More effectively budget for network operations costs
- Reduce system outages and support issues with a proactive plan for replacing aging network components
- Accelerate time to revenue through faster deployment and cutover time when migrating
- Reduce operating expenses
- Introduce new capabilities with potentially lower total cost of ownership.

Manage: Optimize your infrastructure, applications, and service management.

Optimization

Optimization Services help you to optimize your network and IT infrastructure, applications, and service management. They identify gaps, deliver recommendations, and provide expert support so you can:

- Improve the performance, availability, resiliency, and visibility of your network and IT services
- Prepare the network and IT infrastructure for change and more effectively manage change
- Increase your team's self-sufficiency
- Reduce operating costs and improve return on your investments
- Mitigate risks that can compromise the privacy and security of data.

Operations Management

Operations Management Services help you simplify network and IT operations, lower the total cost of network ownership, and accelerate adoption of advanced technologies while retaining visibility and control. By out-tasking proactive monitoring and management of your network infrastructure in alignment with industry standard processes such as ITIL® and eTOM, these can help you:

- Solve problems faster and more effectively manage risk and growth in your network
- Pre-empt incidents and reduce the effects of those that cannot be prevented

- Accelerate adoption of advanced technologies
- Enable a higher quality end-user experience.

Services Pricing Models

Depending on the service that is selected by the customer, Cisco can provide a pricing model that is either a subscription (i.e., prepaid 12-month engagement for a subject matter expert or SMARTnet, among others) or statement of work (transactional) offering (i.e., set deliverables offered at a fixed price).

Under the contract, Cisco is pleased to make available its full portfolio of maintenance and professional services. A full description of each service and service level can be viewed at the following site:

http://www.cisco.com/web/about/doing_business/legal/service_descriptions/index.html#~2

5.3.1.3 Partner Services — Provided by Contractor's Authorized Partners/Resellers.

- Subject to Contractor's approval and the certifications held by its Partners/Resellers, many Partners/Resellers can also offer and provide some or all of the Services as listed above at competitive pricing, along with local presence and support. As the prime, Contractor is still ultimately responsible for the performance of its Partners/ Resellers. Customers can have the option to purchase the Services to be directly delivered by Contractor (OEM) or its certified Partners/Resellers.

Cisco Response:

Read and understood. Subject to Cisco's approval and holding active and applicable certifications, the Authorized Resellers (as selected pursuant to the process as outlined in our response to Section 4.6 above) will be permitted to do the following:

1) Resell Cisco's services that are awarded under this contract and as set forth in Cisco's U.S. Global Price Lists
2) Provide Basic Installation and Configuration Services as follows:

- Certified and Technical Project Management
- Global Implementation Capability
- Staging and Implementation Engineering (Installation)
- Configuration Development
- Site Survey
- Knowledge Transfer
- High Level Design Review
- Acceptance Testing
- Cabling Installation.

**Cisco may modify this list of Partner Services at its discretion.*

Once Cisco vets and selects the Authorized Resellers in accordance with the process as described in our response to Section 4.6 above, we will solicit each Authorized Reseller for their specific onsite and remote hourly rates for each Participating Addendum that they are authorized to resell under, if they wish to provide such services. This process is consistent with our approach today under the current Cisco WSCA Data Communications AR-233 contract in coordination with the State of Utah.

DISCRETIONARY BY CISCO: Cisco's Authorized Resellers may also provide other Professional Services, including hosted services, that Cisco is awarded under the resulting WSCA-NASPO contract; but only on a case-by-case basis to be determined and approved by Cisco, at its sole discretion and subject to Cisco's business, operational, and legal requirements.

5.3.1.4 Training — Learning offerings for IT professionals on networking technologies, including but not limited to designing, implementing, operating, configuring, and troubleshooting network systems pertaining to items provided under the master agreement.

Cisco Response:

To provide WSCA-NASPO customers with access to training and development on Cisco's products and offerings, we are pleased to offer Cisco Learning Credits for purchase under the contract. Cisco Learning Credits are available for purchase on the U.S. Global Price Lists and sold in packages of 10, 100, 500, and 1500. They can be added to any Cisco hardware, software, or solution purchase and redeemed within 1 year from activation on the Cisco Learning Credits Management Tool (LCMT). Cisco Learning Credits can be redeemed for high-quality, authorized training from a Cisco Learning Partner or their affiliated organizations, or Cisco Advanced Services Education.

With Cisco Learning Credits, customers can:

- Realize a faster return on your investment
- Increase overall productivity and network uptime
- Safeguard your training budget and reduce administrative costs
- Assess and keep track of your organization's training needs with the unique LCMT
- Obtain a complete solution that includes Cisco authorized training.

Determining the Number of Cisco Learning Credits to Purchase

Cisco Learning Partners offer a Training Needs Assessment, a consultative, complementary service that helps you identify your network training needs and develop a training plan.

Redeeming Cisco Learning Credits

Cisco Learning Credits are valid for 1 year from activation on LCMT. They can be redeemed for high-quality, authorized training from a Cisco Learning Solutions Partner or their affiliated organizations, or Cisco Advanced Services Education. Each Cisco Learning Credit is worth $100 toward the purchase of Cisco authorized training.

Managing Cisco Learning Credits

Cisco Learning Credits are registered in the LCMT, a unique and easy-to-use online database that keeps track of your Cisco Learning Credits transactions, validates redemptions, and sends monthly statements.

The Value of Cisco Authorized Training through Cisco Learning Partners

Cisco Learning Partners and their affiliated organizations are the only authorized channel sources for Cisco training. As such, they are qualified to deliver customized, market-leading Cisco training that incorporates the latest training content and Cisco intellectual property.

Partner Training

In addition to Cisco Learning Credits and subject to Cisco approval, the Authorized Resellers may add customized training to address specific customer requirements. Once Cisco vets and selects the Authorized Resellers in accordance with the process as described in our response to Section 4.6 above, we will solicit each Authorized Reseller under each Participating Addendum for their specific onsite and remote hourly rates for training, if they wish to provide such services. This process is consistent with our approach today under the current Cisco WSCA Data Communications AR-233 contract in coordination with the State of Utah.

5.3.2 ADDING PRODUCTS

The ability to add new equipment and services is for the convenience and benefit of WSCA-NASPO, the Participating States, and all the Authorized Purchasers. The intent of this process is to promote "one-stop shopping" and convenience for the customers and equally important, to make the contract flexible in keeping up with rapid technological advances. The option to add new product or service categories and/items will expedite the delivery and implementation of new technology solutions for the benefit of the Authorized Purchasers.

After the contracts are awarded, additional IT product categories and/or items may be added per the request of the Contractor, a Participating State, an Authorized Purchaser or WSCA-NASPO. Additions may be ad hoc and temporary in nature or permanent. All additions to an awarded Contractor or Manufacturer's offerings must be products, services, software, or solutions that are commercially available at the time they are added to the contract award and fall within the original scope and intent of the RFP (i.e., converged technologies, value adds to manufacturer's solution offerings, etc.).

Cisco Response:

Read and understood. Please note that depending on the technology, additional terms and conditions may be required.

5.3.2.1 New Product from Contractors — If Contractor, a Participating State, an Authorized Purchaser or WSCA-NASPO itself requests to add new product categories permanently, then all awarded Contractors (Manufacturers) will be notified of the proposed change and will have the opportunity to work with WSCA to determine applicability, introduction, etc. Any new products or services must be reviewed and approved by the WSCA-NASPO Contract Administrator.

Cisco Response:

Read and understood. Please note that depending on the technology, additional terms and conditions may be required.

5.3.2.2 Ad Hoc Product Additions — A request for an ad hoc, temporary addition of a product category/item must be submitted to WSCA-NASPO via the governmental entity's contracting/purchasing officer. Ad hoc, temporary requests will be handled on a case-by-case basis.

Cisco Response:

Read and understood. Please note that depending on the technology, additional terms and conditions may be required.

5.3.2.3 Pricelist Updates — As part of each Contractor's ongoing updates to its pricelists throughout the contract term, Contractor can add new SKUs to its awarded product categories that may have been developed in-house or obtained through mergers, acquisitions or joint ventures; provided, however, that such new SKUs fall within the Contractor's awarded product categories.

Cisco Response:

Read and understood. As stated earlier in Section 1.13, since Cisco's entire U.S. Global Price Lists are refreshed on a monthly basis that includes new SKUs, Cisco wishes to provide updates on a monthly basis under the resulting WSCA-NASPO contract to ensure that Purchasing Entities will have timely access to new SKUs that are available from the awarded product categories.

Note: Depending on the technology, additional terms and conditions may be required.

Section 7: Master Agreement Terms and Conditions/Exceptions

7.1 WSCA-NASPO Master Agreement Terms and Conditions

7.1.1 The WSCA-NASPO Contract Administrator referred to in section 2 of the WSCA-NASPO Master Agreement Terms and Conditions is Debra Gunderson, State of Utah Division of Purchasing and General Services. This RFP represents the WSCA-NASPO Contract Administrator's written approval of the modifications, waivers, alterations, amendments, and supplements to the Master Agreement Terms and Conditions made in this RFP and this Section 7.

Cisco Response:

Read and understood.

7.1.2 Except as limited in this section or elsewhere in this RFP, Participating Entities who execute a Participating Addendum may alter, modify, supplement, or amend the WSCA- NASPO Master Agreement Terms and Conditions as necessary to comply with Participating Entity law or policy with respect to their orders under the Master Agreement. A Contractor may not deliver Products or perform services under this Master Agreement until a Participating Addendum acceptable to the Participating Entity and Contractor is executed. The WSCA-NASPO Terms and Conditions are applicable to any order by a Participating Entity, except to the extent altered, modified, supplemented or amended by a Participating Addendum. By way of illustration and not limitation, this authority may apply to unique delivery and invoicing requirements, confidentiality requirements, defaults on orders, governing law and venue relating to orders by a Participating Entity, Indemnification, and insurance requirements. Statutory or constitutional requirements relating to availability of funds may require specific language in some Participating Addenda in order to comply with applicable law. The expectation is that these alterations, modifications, supplements, or amendments will be addressed in the Participating Addendum or, with the consent of the Participating Entity and Contractor, may be included in the commitment voucher (e.g. purchase order or contract) used by the Participating Entity to place the order.

Cisco Response:

Read and understood.

7.1.3 The term Purchasing Entity and Participating Entity shall both mean "Participating Entity" as that term is defined in WSCA-NASPO Master Agreement Terms and Conditions.

Cisco Response:

Read and understood.

7.1.4 With respect to section 11, Indemnification, the terms of any Participating Addendum may alter, modify, supplement, or amend the language in section 11 and may include a limitation of liability mutually agreeable to the Participating Entity and the Contractor.

Cisco Response:

Read and understood.

7.1.5 With regard to section 20, Participants, Participating Entities who are not states may under some circumstances sign their own Participating Addendum, subject to the approval of the Chief Procurement Official of the state where the Participating Entity is located. Contractors may upon request obtain a copy of the written authorization from the WSCA-NASPO Contract Administrator.

Cisco Response:

Read and understood.

7.2 Offeror Exceptions to Terms and Conditions

7.2.1 The Lead State discourages exceptions to contract terms and conditions in the RFP, attached Participating Entity terms and conditions (if any), and the WSCA-NASPO Master Agreement Terms and Conditions. As specified in this RFP, exceptions may cause a proposal to be rejected as nonresponsive when, in the sole judgment of the Lead State (and its evaluation team), the proposal appears to be conditioned on the exception or correction of what is deemed to be a deficiency or unacceptable exception would require a substantial proposal rewrite to correct. Moreover, Offerors are cautioned that award may be made on receipt of initial proposals without clarification or an opportunity for discussion, and the nature of exceptions would be evaluated. Further, the nature of exceptions will be considered in the competitive range determination if one is conducted. Exceptions will be evaluated to determine the extent to which the alternative language or approach poses unreasonable, additional risk to the state, is judged to inhibit achieving the objectives of the RFP, or whose ambiguity makes evaluation difficult and a fair resolution (available to all vendors) impractical given the timeframe for the RFP.

Cisco Response:

Read and understood. Cisco would greatly appreciate the opportunity to clarify and discuss any of our exceptions. We look forward to working with WSCA-NASPO to reach mutually agreeable terms and conditions. Cisco and WSCA have operated successfully with the current Cisco WSCA Data Communications AR-233 contract for over the last 5 years. These mutually negotiated terms have served all parties well, including the Participating States, which is a testament to the robust and comprehensive nature of the existing agreement. As such, we recommend that certain sections that we utilize the terms of our existing WSCA Data Communications AR-233 contract. This approach will also serve to expedite reaching final agreement on terms and conditions.

7.2.2 The Lead State will entertain exceptions to contract terms and conditions in this RFP, including the WSCA-NASPO Master Agreement Terms and Conditions. Offerors are strongly encouraged to be judicious in identifying exceptions.

Cisco Response:

Read and understood. Cisco and WSCA have operated successfully with the current Cisco WSCA Data Communications AR-233 contract for over the last 5 years. These mutually negotiated terms have served all parties well, including the Participating States, which is a testament to the robust and comprehensive nature of the existing agreement. As such, we recommend that certain sections that we utilize the terms of our existing WSCA Data Communications AR-233 contract. This approach will also serve to expedite reaching final agreement on terms and conditions.

7.2.3 Based on the market research conducted by the Lead State, the following provisions are intended to frame the contours of exceptions that may be acceptable, additional risk so long as the Offeror's exceptions are specified with sufficient particularity.

Cisco Response:

Read and understood.

7.2.4 The Lead State will consider Offeror standard terms for inspection and acceptance, so long as a reasonable time for acceptance is stated. However, the Participating Entities right to exercise revocation of acceptance under its Uniform Commercial Code must be preserved. Submit the standard terms with the offer and describe generally how commerciality in their use is established, e.g., identify publicly-available catalogs where the warranty terms are used and how long they have been in use.

Cisco Response:

As noted in the response to 7.2.1, Cisco and WSCA have operated successfully with the current Cisco WSCA Data Communications AR-233 contract for over the last 5 years. As such, we recommended that

certain sections of the proposed agreement, including acceptance, be continued in any new agreement with Cisco. Cisco's standard terms of Warranty may be found at the following publically available catalog of warranty terms for our products: www.cisco.com/go/warranty.

7.2.5 The Lead State will consider standard warranty and/or maintenance terms, but the alternative warranty and/or maintenance will be evaluated to determine whether they provide comparable protection to the warranty specified in section 30 of the WSCA-NASPO Master Agreement Terms and Conditions. Provide the terms of the warranty and maintenance in the offer. Also describe generally how commerciality is established for those terms, e.g., publicly-available catalogs the warranty terms are used and how long they have been in use. Provide one reference from a customer having comparable sales volume who is using the warranty and maintenance provisions, where the warranty term has expired, and who has exercised rights under the warranty.

Cisco Response:

Read and understood. As noted in the response to 7.2.1, Cisco and WSCA have operated successfully under the warranty terms in the current Cisco WSCA Data Communications AR-233 contract for over the last 5 years. To the best of our knowledge, we are not aware of any customer with comparable sales volume who had exercised rights under the warranty provisions post expiration of the warranty term. As such, we recommend that certain sections of the proposed agreement be continued in any new agreement with Cisco. Cisco's standard terms of Warranty may be found at the following publically available catalog of warranty terms for our products: www.cisco.com/go/warranty.

7.2.6 Intellectual property. The Lead State will consider license terms and conditions that as a minimum convey to Participating Entities a nonexclusive, irrevocable, perpetual, paid-up, royalty free license to use software or other intellectual property delivered with or inherent in the commodity or service, and to transfer the license rights to third parties for government purposes. Provide the terms of the license, including any terms that cover third party intellectual property used in the Offeror's solution. Offerors should be aware that Participating Entities using federal funds may be required to negotiate additional or different terms to satisfy minimum rights requirements of their federal grants.

Cisco Response:

Read and understood. As noted in the response to 7.2.1, Cisco and WSCA have operated successfully with the current Cisco WSCA Data Communications AR-233 contract for over the last 5 years. As such, we recommend that in intellectual property provisions of the existing WSCA Data Communications AR-233 contract be continued in any new agreement with Cisco.

7.2.7 Any limitation of liability provision – including any exclusion of damages clause – proposed by an Offeror to be the default limitation of liability provision under the Master Agreement must preserve a reasonable amount of direct damages for breach of contract, additionally permit the Participating Entity to recoup amounts paid for supplies or services not finally accepted (as in the case of advance or progress payments, if used), and preserve the right of the Participating Entity to be held harmless from costs of litigation as well as ultimate liability within limits agreed by the parties.

Moreover, any limitation of liability clause proposed by an Offeror should be reciprocal, cover lost profits, and exclude claims or liability arising out of intellectual property infringement, bodily injury (including death), damage to tangible property, and data breach. Include the text of any such language if proposed. Further, provide contact information for a public entity, or private entity if no public entity exists, where the limitation of liability clause (or another clause substantially similar) operated to limit liability. If no such example exists, provide contact information for a state, or if no state exists, a higher education institution, or if none exists, a city or county represented by counsel in the negotiations who has agreed to the proposed terms and conditions.

Cisco Response:

Read and understood. As noted in the response to 7.2.1, Cisco and WSCA have operated successfully with the current WSCA Data Communications AR-233 contract for over the last 5 years. As such, we

recommend that limitation of liability in the existing agreement be continued in any new agreement with Cisco. The State of Utah agreed to these terms in the existing WSCA Data Communications AR-233 contract.

7.2.8 The enumerated examples in subsection 7.2 are not intended to limit the ability of Offerors to propose additional, reasonable exceptions. For any other exception, where the exception is based on claims of standard or normal commercial practice, provide contact information for a state, or if no state exists, a higher education institution, or if none exists, a city or county represented by counsel in the negotiations who has agreed to the proposed terms and conditions.

Cisco Response:

Cisco and WSCA have operated successfully with the current Cisco WSCA Data Communications AR-233 contract for over the last 5 years. The State of Utah agreed to these terms in the existing WSCA Data Communications AR-233 contract, as did the Participating States (except where State Statute required modification). These would serve as references to our exceptions.

7.3 WSCA-NASPO eMarket Center

7.3.1 In July 2011, WSCA-NASPO entered into a multi-year agreement with SciQuest, Inc. whereby SciQuest will provide certain electronic catalog hosting and management services to enable eligible WSCA-NASPO entity's customers to access a central online website to view and/or shop the goods and services available from existing WSCA-NASPO Cooperative Contracts. The central online website is referred to as the WSCA-NASPO eMarket Center Contractor shall either upload a hosted catalog into the eMarket Center or integrate a punchout site with the eMarket Center.

Cisco Response:

Read and understood.

Supplier's Interface with the eMarket Center

There is no cost charged by SciQuest to the Contractor for loading a hosted catalog or integrating a punchout site.

At a minimum, the Contractor agrees to the following:

1. Implementation Timeline: WSCA-NASPO eMarket Center Site Admin shall provide a written request to the Contractor to begin enablement process. The Contractor shall have fifteen (15) days from receipt of written request to work with WSCA-NASPO and SciQuest to set up an enablement schedule, at which time SciQuest's technical documentation shall be provided to the Contractor. The schedule will include future calls and milestone dates related to test and go live dates. The contractor shall have a total of Ninety (90) days to deliver either a (1) hosted catalog or (2) punch-out catalog, from date of receipt of written request.

Cisco Response:

Cisco will work with SciQuest to enable the pricelist implementation. However, because Cisco's entire U.S. Global Price Lists will be very large with respect to the products and services categories listed in this RFP (i.e., 700,000+ SKUs), we anticipate that there may be some implementation challenges given the size of Cisco's offerings. Therefore, we are respectfully requesting that WSCA-NASPO allows Cisco to work with Sci-Quest first in determining a reasonable implementation schedule based on our situation and potential issues, which may exceed ninety (90) days to test and go live. Since we are not familiar with the SciQuest tool, we are uncertain if there will any limitations or issues with their tool in handling the potential size of Cisco's U.S. Global Price Lists.

2. Definition of Hosted and Punchout: WSCA-NASPO and SciQuest will work with the Contractor, to decide which of the catalog structures (either hosted or punch-out as further described below) shall be provided by the Contractor. **Whether hosted or punch-out, the catalog must be strictly limited to the Contractor's awarded contract offering (e.g. products and/or services**

not authorized through the resulting cooperative contract should not be viewable by WSCA-NASPO Participating Entity users).

a. Hosted Catalog. By providing a hosted catalog, the Contractor is providing a list of its awarded products/services and pricing in an electronic data file in a format acceptable to SciQuest, such as Tab Delimited Text files. In this scenario, the Contractor must submit updated electronic data annually to the the eMarket Center for WSCA-NASPO Contract Administrator's approval to maintain the most up-to-date version of its product/service offering under the cooperative contract in the eMarket Center.

b. Punch-Out Catalog. By providing a punch-out catalog, the Contractor is providing its own online catalog, which must be capable of being integrated with the eMarket Center as a. Standard punch-in via Commerce eXtensible Markup Language (cXML). In this scenario, the Contractor shall validate that its online catalog is up-to-date by providing a written update quarterly to the Contract Administrator stating they have audited the offered products/services and pricing listed on its online catalog. The site must also return detailed UNSPSC codes (as outlined in line 3) for each line item. Contractor also agrees to provide e-Quote functionality to facilitate volume discounts.

Cisco Response:

Because Cisco's technologies are not off-the-shelf purchasable items, they have to be individually configured. Consequently, we will be pursuing the Hosted Catalog structure with SciQuest since the Punch-Out catalog model is not a viable option for us. However, we would still need to understand the exact format to execute the Hosted catalog structure for Cisco's U.S. Global Price Lists. In addition, as discussed in our response to Section 1.13, Cisco is respectfully requesting the ability to update/refresh our pricebooks on a monthly basis for the awarded items to ensure that our customers have access to the latest options and pricing available for the awarded categories. Cisco is very responsive to the rapid market changes in the Data Communications space. Therefore, it is our practice to update our U.S. Global Price Lists on a monthly basis to include ongoing enhancements, improvements, service coverage options, special pricing bundles, new spare parts, and new technological advances. In a world that is changing rapidly, Cisco strongly believes in enabling governments to have timely access and options to new technologies and business practices so that smart investments are made to improve and enrich the lives of their citizens.

3. Revising Pricing and Product Offerings: Any revisions (whether an increase or decrease) to pricing or product/service offerings (new products, altered SKUs, etc.) must be pre-approved by the WSCA-NASPO Contract Administrator and shall be subject to any other applicable restrictions with respect to the frequency or amount of such revisions. However, no cooperative contract enabled in the eMarket Center may include price changes on a more frequent basis than once per quarter. The following conditions apply with respect to hosted catalogs:

Cisco Response:

Cisco is agreeable that any revisions to pricing (increase or decrease) or product/service offerings (new and removed products, altered SKUs, etc.) will need to be pre-approved by the WSCA-NASPO Contract Administrator. However, Cisco respectfully requests to take an exception to the price changes not being allowed on a more frequent basis than once per quarter. As stated earlier in Section 1.13 and Section 1.14, since Cisco's entire U.S. Global Price Lists are refreshed on a monthly basis that includes price changes, addition of new SKUs and removal of SKUs, Cisco wishes to provide updates on a monthly basis under the resulting WSCA-NASPO contract.

a. Updated pricing files are required by the 1st of the month and shall go into effect in the eMarket Center on the 1st day of the following month (i.e. file received on 1/01/14 would be effective in the eMarket Center on 2/01/14). Files received after the 1st of the month may be delayed up to a month (i.e. file received on 11/06/14 would be effect in the eMarket Center on 1/01/15).

Cisco Response:

Read and understood. Cisco is agreeable to submitting the updated files by the 1st of each month, but would hope that SciQuest can process the updates in the eMarket Center as soon as possible. As discussed earlier, delays in posting updated pricelists could materially affect the Purchasing Entity's ability to procure up-to-date Cisco products and services that would best suit their short-term and long-term needs.

b. Contract Administrator-approved price changes are not effective until implemented within the eMarket Center. Errors in the Contractor's submitted pricing files will delay the implementation of the price changes in eMarket Center.

Cisco Response:

Read and understood.

4. Supplier Network Requirements: Contractor shall join the SciQuest Supplier Network (SQSN) and shall use the SciQuest's Supplier Portal to import the Contractor's catalog and pricing, into the SciQuest system, and view reports on catalog spend and product/pricing freshness. The Contractor can receive orders through electronic delivery (cXML) or through low-tech options such as fax. More information about the SQSN can be found at: www.sciquest.com or call the SciQuest Supplier Network Services team at 800-233-1121.

Cisco Response:

Cisco is respectfully taking exception to this requirement. Cisco products must be configured in and ordered through Cisco's tools by our Authorized Resellers. We are requesting that the ordering process under the current WSCA Data Communications AR-233 contract remain in effect. That is, Purchasing Entities under each Participating Addendum would place orders directly with Cisco's Authorized Resellers. Upon acceptance, the Authorized Resellers would process the orders from end-to-end, including ensuring delivery of the orders, invoicing and receiving payments from the Purchasing Entities under the terms and conditions of the resulting WSCA-NASPO Master Agreement and the applicable Participating Addendum.

5. Minimum Requirements: Whether the Contractor is providing a hosted catalog or a punch-out catalog, the Contractor agrees to meet the following requirements:

   a. Catalog must contain the most current pricing, including all applicable administrative fees and/or discounts, as well as the most up-to-date product/service offering the Contractor is authorized to provide in accordance with the cooperative contract; and

   b. The accuracy of the catalog must be maintained by Contractor throughout the duration of the cooperative contract between the Contractor and the Contract Administrator; and

   c. The Catalog must include a Lead State contract identification number; and

   d. The Catalog must include detailed product line item descriptions; and

   e. The Catalog must include pictures when possible; and

   f. The Catalog must include any additional WSCA-NASPO and Participating Addendum requirements.*

Cisco Response:

Read and understood.

6. Order Acceptance Requirements: Contractor must be able to accept Purchase Orders via fax or cXML.

   a. The Contractor shall provide positive confirmation via phone or email within 24 hours of the Contractor's receipt of the Purchase Order. If the Purchasing Order is received after 3pm

EST on the day before a weekend or holiday, the Contractor must provide positive confirmation via phone or email on the next business day.

Cisco Response:

Cisco is respectfully taking exception to this section. As discussed earlier, our Authorized Resellers vary in size and resources. Although many are small to medium size businesses, they are strategically selected to be Cisco's subcontractors because of the great value add they bring in supporting our WSCA-NASPO customers with their Cisco expertise and economic development in each Participating State/Entity. Because we anticipate that the qualification profile and make-up of the Authorized Resellers to be similar with the set of partners we have today under the current WSCA Data Communications AR-233 contract, we are requesting that the confirmation requirement for purchase orders be forty-eight (48) hours via phone or email instead to give some consideration to these small and medium size Cisco resellers.

7. UNSPSC Requirements: Contractor shall support use of the United Nations Standard Product and Services Code (UNSPSC). UNSPSC versions that must be adhered to are driven by SciQuest for the suppliers and are upgraded every year. WSCA-NASPO reserves the right to migrate to future versions of the UNSPSC and the Contractor shall be required to support the migration effort. All line items, goods or services provided under the resulting statewide contract must be associated to a UNSPSC code. All line items must be identified at the most detailed UNSPSC level indicated by segment, family, class and commodity. More information about the UNSPSC is available at: http://www.unspsc.com and http://www.unspsc.com/FAQs.asp#howdoesunspscwork.

Cisco Response:

Cisco would like to take exception to this requirement due to the size and frequency of Cisco's U.S. Global Price Lists updates, including for the U.S. market. It would be extremely arduous for us to assign these UNSPSC codes to each specific part or SKU#. As stated previously in 7.3.1, there are over 700,000 lines (SKUs) in the original price lists that are being submitted with this RFP, and then going forward, we anticipate 10,000 to 20,000 new product and service items being added monthly in order to keep abreast of the market for Data Communications technologies and services as set forth in this RFP.

8. Applicability: Contractor agrees that WSCA-NASPO controls which contracts appear in the eMarket Center and that WSCA-NASPO may elect at any time to remove any supplier's offering from the eMarket Center.

Cisco Response:

Read and understood. However, Cisco is requesting that it be provided ten (10) business days advance written notice of any removal and the reason(s) for such. We would also appreciate the opportunity to appeal any removal decision and have the offering re-instated if both parties are in agreement.

9. The WSCA-NASPO Contract Administrator reserves the right to approve the pricing on the eMarket Center. This catalog review right is solely for the benefit of the WSCA-NASPO Contract Administrator and Participating Entities, and the review and approval shall not waive the requirement that products and services be offered at prices (and approved fees) required by the Master Agreement.

   *Although suppliers in the SQSN normally submit one (1) catalog, it is possible to have multiple contracts applicable to different WSCA-NASPO Participating Entities. For example, a supplier may have different pricing for state government agencies and Board of Regents institutions. Suppliers have the ability and responsibility to submit separate contract pricing for the same catalog if applicable. The system will deliver the appropriate contract pricing to the user viewing the catalog.

   Several WSCA-NASPO Participating Entities currently maintain separate SciQuest eMarketplaces, these Participating Entities do enable certain WSCA-NASPO Cooperative

Contracts. In the event one of these entities elects to use this WSCA-NASPO Cooperative Contract (available through the eMarket Center) but publish to their own eMarketplace, the Contractor agrees to work in good faith with the entity and WSCA-NASPO to implement the catalog. WSCA-NASPO does not anticipate that this will require substantial additional efforts by the Contractor; however, the supplier agrees to take commercially reasonable efforts to enable such separate SciQuest catalogs.

Cisco Response:

Read and understood.

Appendix A — WSCA-NASPO Terms and Conditions with Noted Exceptions

Cisco Comment: Cisco and WSCA have operated successfully with the current terms and conditions for over the last 5 years. As such, we recommend in certain sections that we utilize the terms of our existing agreement. These terms have served all parties well, including the Participating States, which serves as a testament to the robust and comprehensive nature of the existing agreement. This approach will also serve to expedite reaching final agreement on terms and conditions.

WSCA-NASPO Master Agreement Terms and Conditions

1. AGREEMENT ORDER OF PRECEDENCE:

The Master Agreement shall consist of the following documents:

1. A Participating Entity's Participating Addendum ("PA");
2. WSCA-NASPO Master Agreement Terms and Conditions (the "Agreement" or "Master Agreement");
3. The Statement of Work;
4. The Solicitation; and
5. Contractor's response to the Solicitation.

These documents shall be read to be consistent and complementary. Any conflict among these documents shall be resolved by giving priority to these documents in the order listed above. Contractor terms and conditions that apply to this Master Agreement are only those that are expressly accepted by the Lead State and must be in writing and attached to this Master Agreement as an Exhibit or Attachment. No other terms and conditions shall apply, including terms and conditions listed in the Contractor's response to the Solicitation, or terms listed or referenced on the Contractor's website, in the Contractor quotation/sales order or in similar documents subsequently provided by the Contractor.

Cisco Response: Agreed. Cisco requests that language regarding the term of the Master Agreement and Effective Date (date of last signature) be added to this Section.

2. AMENDMENTS The terms of this Master Agreement shall not be waived, altered, modified, supplemented or amended in any manner whatsoever without prior written approval of the WSCA-NASPO Contract Administrator.

Cisco Response: Agreed, with the provision that there will be mutual written approval before any terms are changed.

3. ASSIGNMENT/SUBCONTRACT Contractor shall not assign, sell, transfer, subcontract or sublet rights, or delegate responsibilities under this contract, in whole or in part, without the prior written approval of the WSCA-NASPO Contract Administrator.

Cisco Response: Cisco respectfully requests that this section be replaced with the terms in the current Cisco WSCA Data Communications AR-233 contract as copied below.

Neither party shall assign, sell, or transfer its rights and responsibilities under this Master Agreement (other than the right to receive any amount due, which shall be freely assignable upon written notice to customer), in whole or in part, without the prior written approval of the other party, which approval will not be unreasonably withheld. Notwithstanding the foregoing, Contractor shall have the right to assign all or part of this Master Agreement as part of a merger, corporate reorganization, or sale of assets or to a

majority-owned or majority-controlled subsidiary or affiliate and to subcontract services to third parties provided that Contractor remains responsible for the performance of such services by subcontractors done in the normal course of their business obligations and duties to Contractor. However, in all cases notwithstanding subcontracting, the customer shall deal only with invoices and payment through either Contractor or the Fulfillment Partners listed on the individual Participating Addendum. Any allowed assignee or merged entity shall be subject to all the terms of this Master Agreement.

Contractor may, with prior written consent from Participating States, which consent shall not be unreasonably withheld, enter into subcontracts with third parties as "Fulfillment Partners." Fulfillment Partners are Subcontractors who may provide p and services under this Master Agreement at the price discounts established in this Master Agreement and bill purchasers directly for such products and services.

Fulfillment Partners, where directed by Contractor, are required to report to the WSCA Contract Manager, account for and submit the WSCA Contract Administration Fee, along with Contract Activity Reports.

Contractor, as well as Fulfillment Partners, participate in the Federal Communication Commission's E-rate discount program established under the authority of the Federal Telecommunications Commission Act of 1996 and may accept and process E-Rate transactions under their own E-rate registration numbers.

4. CANCELLATION Unless otherwise stated in the special terms and conditions, any Master Agreement may be canceled by either party upon 60 days notice, in writing, prior to the effective date of the cancellation. Further, any Participating State may cancel its participation upon 30 days written notice, unless otherwise limited or stated in the special terms and conditions of this solicitation. Cancellation may be in whole or in part. Any cancellation under this provision shall not effect the rights and obligations attending orders outstanding at the time of cancellation, including any right of and Purchasing Entity to indemnification by the Contractor, rights of payment for goods/services delivered and accepted, and rights attending any warranty or default in performance in association with any order. Cancellation of the Master Agreement due to Contractor default may be immediate.

Cisco Response: Per our understanding of the Q&A prior to contract submission, it appears that the "Special Terms and Conditions" are this document. If this understanding is correct, please delete "Unless otherwise stated in the Special Terms and Conditions."

Please change the last sentence to the following: *Cancellation of the Master Agreement due to <u>either party's</u> default may be immediate.*

In addition, Cisco respectfully requests the following addition from the current Cisco WSCA Data Communications AR-233 contract.

On termination, all accounts and payments will be processed according to the financial arrangements set forth herein for products delivered and/or approved services rendered to date of termination.

Rights upon Termination or Expiration

1. *Upon termination or expiration of this contract or a Participating Addendum, (a) Contractor reserves the right to cease all further delivery of product or services, (b) all outstanding invoices become due and payable within thirty (30) days of termination, and (c) all rights and licenses of customer under this contract shall terminate. If Contractor agrees to complete delivery of any further products or services due against any existing accepted Purchase Orders, then customer shall pay for such products or services in advance within thirty (30) days.*
2. *Except for a termination of this contract resulting from customer's breach of Contractor's proprietary rights and software licensing, Confidential Information, or Export, Re-Export, Transfer and Use Controls, upon termination or expiration of this contract, customer may continue to use, in accordance with the terms and conditions of this contract and/or the Participating Addendum, products provided to it by Contractor prior to the date of termination or expiration provided payment has been made in full for such products.*
3. *Upon termination or expiration of this contract, customer shall immediately return to Contractor all Confidential Information (including all copies thereof) then in State's possession, custody, or control (except that State may retain one archival copy for records retention purposes only as required by law); provided that, except for a termination resulting from customer's breach of*

proprietary rights and software licensing, Confidential Information, or Export Restrictions, customer may retain a sufficient amount of such Confidential Information and material to operate its installed base of products.

4. *In the event of any termination pursuant to this section, and unless otherwise required by law or court of competent jurisdiction, customer shall remain obligated to comply in perpetuity with the provisions of Contractor's Software License terms, Export Restrictions, and Confidential Information for purchased product.*

5. CONFIDENTIALITY, NON-DISCLOSURE AND INJUNCTIVE RELIEF

5.1 Confidentiality. Contractor acknowledges that it and its employees or agents may, in the course of providing the Product under this Master Agreement, be exposed to or acquire information that is confidential to Participating Entity or Participating Entity's clients. Any and all information of any form that is marked as confidential or would by its nature be deemed confidential obtained by Contractor or its employees or agents in the performance of this Master Agreement, including, but not necessarily limited to (a) any Participating Entity records, (b) personnel records, and (c) information concerning individuals, is confidential information of Participating Entity ("Confidential Information"). Any reports or other documents or items (including software) that result from the use of the Confidential Information by Contractor shall be treated in the same manner as the Confidential Information. Confidential Information does not include information that (a) is or becomes (other than by disclosure by Contractor) publicly known; (b) is furnished by Participating Entity to others without restrictions similar to those imposed by this Master Agreement; (c) is rightfully in Contractor's possession without the obligation of nondisclosure prior to the time of its disclosure under this Master Agreement; (d) is obtained from a source other than Participating Entity without the obligation of confidentiality, (e) is disclosed with the written consent of Participating Entity or; (f) is independently developed by employees, agents or subcontractors of Contractor who can be shown to have had no access to the Confidential Information.

Cisco Response: Cisco respectfully requests that this Section be replaced with the following from the Cisco WSCA Data Communications AR-233 contract, which is a mutual provision.

Notwithstanding anything contained in the Master Agreement to the contrary, the following shall govern the obligations with respect to Confidential Information under this Master Agreement.

5.1. *Definitions.*

5.1.1. Customer "Confidential Information" includes information regarding Customer's network operations, technical architecture, operations, and plans and security data.

5.1.2. Contractor "Confidential Information" includes information regarding Contractor's hardware, software and service products, technical, financial and marketing data, and information posted on password protected areas on www.cisco.com.

5.1.3. Information (other than that on www.cisco.com) disclosed by the disclosing party in written or other tangible form will be considered Confidential Information only if it is clearly marked "Confidential," "Proprietary," or with a similar legend, which wording the parties hereby agree constitutes acceptable and equivalent marking and protective notice to satisfy and invoke initial protection of the local Freedom of Information Laws applicable to a Purchaser under a Participating Addendum.

5.1.4. Information disclosed orally shall only be considered Confidential Information if: (i) identified as confidential, proprietary or the like at the time of disclosure, and (ii) confirmed in writing within thirty (30) days of disclosure.

5.1.5. Confidential Information disclosed to the receiving party by any Affiliate or agent of the disclosing party is subject to this Master Agreement.

5.2. *The receiving party may use the Confidential Information solely in furtherance of the objectives of this Master Agreement.*

5.3. *Except as set forth in subsection 4 below, neither party shall disclose the Confidential Information to any third party.*

5.4. *The receiving party may disclose Confidential Information to its employees, subcontractors, or Affiliates' employees and subcontractors only: (a) on a "need to know" basis, (b) consistent with the objectives of this Master Agreement, and (c) pursuant to separate written non-disclosure terms that contractually obligate such employees and subcontractors to maintain the confidentiality of the Confidential Information.*

5.5. *Notwithstanding any other provision in this Master Agreement, the receiving party shall have no obligation with respect to information which:*

5.5.1. was rightfully in possession of or known to the receiving party without any obligation of confidentiality prior to receiving it from the disclosing party;

5.5.2. is, or subsequently becomes, legally and publicly available without breach of this Master Agreement;

5.5.3. is rightfully obtained by the receiving party from a source other than the Disclosing Party without any obligation of confidentiality;

5.5.4. is developed by or for the receiving party without use of the Confidential Information and such independent development can be shown by documentary evidence;

5.5.5. is disclosed by the receiving party pursuant to a valid order issued by a court or government agency, provided that the receiving party provides (1) prior written notice to the disclosing party of such obligation and (2) the opportunity to oppose such disclosure.

5.6. *Upon written notification by the disclosing party, the receiving party shall (i) cease using the Confidential Information and (ii) if requested to do so, and to the extent permitted by Customer's applicable records laws, either return it to the disclosing party or destroy it, along with all copies, notes, or extracts thereof and certify to its destruction within fifteen (15) days of receipt of such notice.*

5.7. *Each party shall retain all right, title, and interest to its own Confidential Information. By conveying Confidential Information, the disclosing party does not grant any license under any trademark, patent, or copyright, or application for same, which is now or thereafter may be obtained by such party.*

5.8. *The receiving party shall not reverse-engineer, decompile, or disassemble any software or remove, overprint, or deface any notice of copyright, trademark, logo, legend, or other notices of ownership from any originals or copies of Confidential Information disclosed to it.*

5.9. *EXCEPT AS TO THE EXPRESS WARRANTIES PROVIDED ELSEWHERE IN THIS MASTER AGREEMENT, CONFIDENTIAL INFORMATION IS PROVIDED "AS IS" WITH ALL FAULTS AND IN NO EVENT, SHALL THE DISCLOSING PARTY BE LIABLE FOR THE ACCURACY OR COMPLETENESS OF THE CONFIDENTIAL INFORMATION.*

5.10. *Notwithstanding termination of this Master Agreement as described herein, the obligations of the receiving party with respect to Confidential Information received prior to termination shall continue for three (3) years from the date the Confidential Information was received.*

5.11. *In the event of any threatened or actual breach of any of the obligations hereunder, a disclosing party may seek injunctive relief, in addition to any other available legal or equitable remedies.*

5.12. *Customer agrees that aspects of the Software and associated documentation, including the specific design and structure of individual programs, constitute trade secrets and/or copyrighted material of Contractor. Customer shall not: disclose, provide, or otherwise make available, such trade secrets or copyrighted material, in any form to any third party, without the prior written consent of Contractor. Customer shall implement reasonable security measures to protect such trade secrets and copyrighted material. Title to Software and documentation shall remain solely with Contractor.*

5.13. *Accordingly, the Software and associated documentation shall not be disclosed to any third party without first notifying Contractor and affording Contractor the opportunity, as allowed by*

law, to seek judicial protection from disclosure of such confidential, trade secret, and proprietary information to a third party.

5.2 Non-Disclosure. Contractor shall hold Confidential Information in confidence, using at least the industry standard of confidentiality, and not to copy, reproduce, sell, assign, license, market, transfer or otherwise dispose of, give, or disclose Confidential Information to third parties or use Confidential Information for any purposes whatsoever other than the performance of this Master Agreement to Participating Entity hereunder, and to advise each of its employees and agents of their obligations to keep Confidential Information confidential. Contractor shall use commercially reasonable efforts to assist Participating Entity in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the generality of the foregoing, Contractor shall advise Participating Entity immediately if Contractor learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Master Agreement and Contractor shall at its expense cooperate with Participating Entity in seeking injunctive or other equitable relief in the name of Participating Entity or Contractor against any such person. Except as directed by Participating Entity, Contractor will not at any time during or after the term of this Master Agreement disclose, directly or indirectly, any Confidential Information to any person, except in accordance with this Master Agreement, and that upon termination of this Master Agreement or at Participating Entity's request, Contractor shall turn over to Participating Entity all documents, papers, and other matter in Contractor's possession that embody Confidential Information. Notwithstanding the foregoing, Contractor may keep one copy of such Confidential Information necessary for quality assurance, audits and evidence of the performance of this Master Agreement.

Cisco Response: With the suggestion of adding the language from the current Cisco WSCA Data Communications AR-233 contract which covers the topics of this Section, this Section may be deleted**.**

5.3 Injunctive Relief. Contractor acknowledges that breach of this Section, including disclosure of any Confidential Information, will cause irreparable injury to Participating Entity that is inadequately compensable in damages. Accordingly, Participating Entity may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies that may be available. Contractor acknowledges and agrees that the covenants contained herein are necessary for the protection of the legitimate business interests of Participating Entity and are reasonable in scope and content.

Cisco Response: With the suggestion of adding the language from the current Cisco WSCA Data Communications AR-233 contract which covers the topics of this Section, this Section may be deleted**.**

6. <u>DEBARMENT</u> The contractor certifies that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction (contract) by any governmental department or agency. If the contractor cannot certify this statement, attach a written explanation for review by WSCA-NASPO.

Cisco Response: Agreed.

7. <u>DEFAULTS & REMEDIES</u>

a. The occurrence of any of the following events shall be an event of default under this Master Agreement:

i. Nonperformance of contractual requirements; or

ii. A material breach of any term or condition of this Master Agreement; or

iii. Any representation or warranty by Contractor in response to the solicitation or in this Master Agreement proves to be untrue or materially misleading; or

iv. Institution of proceedings under any bankruptcy, insolvency, reorganization or similar law, by or against Contractor, or the appointment of a receiver or similar officer for Contractor or any of its property, which is not vacated or fully stayed within thirty (30) calendar days after the institution or occurrence thereof; or

v. Any default specified in another section of this Master Agreement.

Cisco Response: Agreed, with a modification of Section ii to "A material breach of a material term or condition of this Master Agreement."

b. Upon the occurrence of an event of default, Lead State shall issue a written notice of default, identifying the nature of the default, and providing a period of 15 calendar days in which Contractor shall have an opportunity to cure the default. The Lead State shall not be required to provide advance written notice or a cure period and may immediately terminate this Master Agreement in whole or in part if the Lead State, in its sole discretion, determines that it is reasonably necessary to preserve public safety or prevent immediate public crisis. Time allowed for cure shall not diminish or eliminate Contractor's liability for damages, including liquidated damages to the extent provided for under this Master Agreement.

Cisco Response: Cisco respectfully requests that this Section be replaced with the following from the current Cisco WSCA Data Communications AR-233 contract.

7.1 Master Agreement: The Lead State or Contractor may terminate this Master Agreement if either party breaches the terms of the Master Agreement as follows: (a) immediately upon providing written notice to the breaching party if the breach is not capable of being cured, and (b) sixty (60) calendar days after providing written notice to the breaching party if the breaching party otherwise fails to cure a material breach within such sixty (60) calendar day period or commence cure within such sixty (60) calendar day period or diligently pursue completion of such cure.

Notwithstanding the foregoing, the Master Agreement may be terminated immediately by Contractor for cause in the event of Purchaser's breach of the provisions relating to Software License, Export Restrictions, or Confidential Information.

7.2 Participating Addendum: If either party to a Participating Addendum (including the Lead State when acting in its sovereign capacity under this Master Agreement) materially breaches any of the provisions of a Participating Addendum, the non-breaching party may terminate the Participating Addendum as follows: (a) immediately upon providing written notice to the breaching party if the breach is not capable of being cured, and (b) thirty (30) calendar days after providing written notice to the breaching party if the breaching party fails to cure such breach within such thirty (30) calendar day period. Notwithstanding the foregoing, a Participating Addendum may be terminated immediately by Contractor for cause in the event of Purchaser's breach of the provisions relating to Software License, Export Restrictions, or Confidential Information.

The cure periods stated in the above paragraph shall not apply to any failure(s) to perform that result from the willful or negligent acts or omissions of the aggrieved party.

c. If Contractor is afforded an opportunity to cure and fails to cure the default within the period specified in the written notice of default, Contractor shall be in breach of its obligations under this Master Agreement and Lead State shall have the right to exercise any or all of the following remedies:

i. Exercise any remedy provided by law; and
ii. Terminate this Master Agreement and any related Contracts or portions thereof; and
iii. Impose liquidated damages as provided in this Master Agreement; and
iv. Suspend Contractor from receiving future bid solicitations; and
v. Suspend Contractor's performance; and
vi. Withhold payment until the default is remedied.

Cisco Response: Agreed with the following modifications:

If Contractor is afforded an opportunity to cure and fails to cure a material default within the period specified in this Master Agreement, Contractor shall be in breach of its obligations under this Master Agreement and Lead State shall have the right to exercise any or all of the following remedies:

i. Exercise any remedy provided by law; and
ii. Terminate this Master Agreement and any related Contracts or portions thereof; and
iii. Suspend Contractor from receiving future bid solicitations; and
iv. Suspend Contractor's performance.

d. In the event of a default under a Participating Addendum, a Participating Entity shall provide a written notice of default as described in this section and have all of the rights and remedies under this paragraph

regarding its participation in the Master Agreement, in addition to those set forth in its Participating Addendum.

Cisco Response: With the suggested addition from the current Cisco WSCA Data Communications AR-233 contract that covers the Participating Addendum, Cisco suggests deletion of this Section.

Please add the following as a replacement to this Section:

Limitation of Liability*. Except for those obligations under Intellectual Property Infringement General Indemnity, notwithstanding anything else herein, all liability of Contractor and its suppliers to any Purchaser for claims arising under this Agreement, the applicable Participating Addendum, or otherwise shall be limited to the money paid to Contractor for Products or for Services with respect to such Purchaser during the twelve (12) month period preceding the event or circumstances giving rise to such liability. This limitation of liability is cumulative and not per incident.*

Waiver of Consequential and Other Damages*. In no event shall Contractor or its suppliers be liable for any incidental, special, indirect, or consequential damages, lost revenue, lost profits, or lost or damaged data, whether arising in contract, tort (including negligence), or otherwise, even if Contractor or its suppliers have been informed of the possibility thereof.*

8. DELIVERY Unless otherwise indicated in the Master Agreement, the prices are the delivered price to any Participating State agency or political subdivision. All deliveries shall be F.O.B. destination with all transportation and handling charges paid by the contractor. Responsibility and liability for loss or damage shall remain the Contractor until final inspection and acceptance when responsibility shall pass to the Buyer except as to latent defects, fraud and Contractor's warranty obligations. The minimum shipment amount will be found in the special terms and conditions. Any order for less than the specified amount is to be shipped with the freight prepaid and added as a separate item on the invoice. Any portion of an order to be shipped without transportation charges that is back ordered shall be shipped without charge.

Cisco Response: Cisco respectfully requests that this Section be replaced with the following from the current Cisco WSCA Data Communications AR-233 contract and that this Section be retitled "Shipping and Delivery."

8.1 After receipt and acceptance by Contractor of Customer's Order(s), Contractor will use commercially reasonable efforts to ship all direct orders designated for shipment to U.S. locations within thirty (30) days for all products. Please note that the following circumstances may affect lead times: (i) new products purchased within the first three (3) months of release of the product which are subject to Contractor's then current published lead-times, (ii) third-party stand-alone products which are not a component of equipment resold by Contractor, (iii) end-of-life products where the termination of the product has been announced by Contractor, (iv) products which have been line-stopped due to software discrepancies, reconfiguration, industry-wide product shortages, or alleged infringement claims, or (vi) situations where government rated orders create delays in lead-times.

Notwithstanding the foregoing, at any time when Customer states "expedite" on an order or otherwise communicates to Contractor that an order is to be expedited, Contractor shall use all commercially reasonable efforts to ensure the earliest possible delivery of such products.

8.2 Contractor will communicate scheduled shipping dates in the order acknowledgement and/or on www.cisco.com within three (3) business days after receipt of an electronic order on www.cisco.com, provided, however, that in the event such notification is not received in this time period, Customer shall notify Contractor of the non-receipt, and Contractor's sole obligation with respect to such non-receipt shall be to promptly provide the information to the Customer after such notification.

8.3 If Contractor has reason to believe that the actual shipment date will occur later than the original shipment date acknowledged by Contractor for reasons caused by Contractor, Contractor shall use commercially reasonable efforts to promptly provide additional information to Customer including by electronic posting of the expected period of delay and, upon request, of the steps available, if any, to minimize the delay. If the extended delivery date is anticipated to be more

than thirty (30) calendar days beyond the originally scheduled delivery date, the parties will work in good faith to resolve any ordering issues pursuant to the order escalation process.

8.4 Shipping terms are FOB destination, shipping and handling prepaid by Contractor. The method of shipment shall be consistent with the nature of the products and hazards of transportation. Acceptance by Customer shall be deemed to have occurred upon delivery of the applicable products to the applicable Customer. Title and risk of loss shall pass to Customer upon delivery.

8.5 If Customer requests delivery of products to Customer's forwarding agent or other representative, Customer assumes responsibility for compliance with applicable export laws and regulations.

8.6 Contractor is not liable for damage or penalty for delay in delivery or for failure to give notice of delay. Contractor shall not have any liability in connection with product shipment other than as set forth in this Section.

All sales are final. Except as provided in Contractor's Limited Warranty, Contractor only permits the return of un-opened products due to Contractor's shipping or order processing error, or damage in transit. No other returns are authorized under this Master Agreement. Warranty returns will not be subject to any restocking charges.

9. <u>FORCE MAJEURE</u> Neither party to this Master Agreement shall be held responsible for delay or default caused by fire, riot, acts of God and/or war which is beyond that party's reasonable control. WSCA-NASPO may terminate this Master Agreement after determining such delay or default will reasonably prevent successful performance of the Master Agreement.

Cisco Response: Cisco respectfully requests replacing this Section with the language from the current Cisco WSCA Data Communications AR-233 contract:

Except for the obligation to pay monies due and owing, neither party shall be liable for any delay or failure in performance due to events outside the defaulting party's reasonable control, including, without limitation, acts of God, earthquake, labor disputes, shortages of supplies, actions of governmental entities, riots, war, terrorism, fire, epidemics, or delays of common carriers. The obligations and rights of the excused party shall be extended on a day-by-day basis for the time period equal to the period of the excusable delay. When payments are delayed solely due to a force majeure event, late fees with respect to such payment will not accrue during the period of such force majeure event.

10. <u>GOVERNING LAW</u> This procurement and the resulting agreement shall be governed by and construed in accordance with the laws of the state sponsoring and administering the procurement. The construction and effect of any Participating Addendum or order against the Master Agreement(s) shall be governed by and construed in accordance with the laws of the Participating Entity's State. Venue for any claim, dispute or action concerning an order placed against the Master Agreement(s) or the effect of an Participating Addendum shall be in the Purchasing Entity's State.

Cisco Response: Agreed, with the 1) correction of "an" to "a" in the last sentence and 2) addition of *"The parties specifically disclaim the application of the U.N. Convention on Contracts for the International Sale of Goods."*

11. <u>INDEMNIFICATION</u> The Contractor shall defend, indemnify and hold harmless WSCA-NASPO, the Lead State and Participating Entities along with their officers, agencies, and employees as well as any person or entity for which they may be liable from and against claims, damages or causes of action including reasonable attorneys' fees and related costs for any death, injury, or damage to property arising from act(s), error(s), or omission(s) of the Contractor, its employees or subcontractors or volunteers, at any tier, relating to the performance under the Master Agreement. This section is not subject to any limitations of liability in this Master Agreement or in any other document executed in conjunction with this Master Agreement

Cisco Response: Cisco respectfully requests replacing this Section with the language from the current Cisco WSCA Data Communications AR-233 contract:

Each party to this Agreement shall defend, indemnify, and hold harmless the other, its corporate affiliates and their respective officers, directors, employees, and agents and their respective successors and assigns from and against any and all claims, losses, liabilities, damages, and expenses (including, without limitation, reasonable attorneys' fees), including without limitation those

based on contract or tort, arising out of or in connection with a claim, suit, or proceeding brought by a third party based upon bodily injury (including death) or damage to tangible personal property (not including lost or damaged data) arising from the negligent or intentional acts or omissions of the indemnifying party or its subcontractors, or the officers, directors, employees, agents, successors, and assigns of any of them. In the event that the indemnified party's or a third party's negligent or intentional acts or omissions contributed to cause the injury or damage for which a claim of indemnity is being asserted against the indemnifying party hereunder, the damages and expenses (including, without limitation, reasonable attorneys' fees) shall be allocated or reallocated, as the case may be, between the indemnified party, the indemnifying party, and any other party bearing responsibility in such proportion as appropriately reflects the relative fault of such parties, or their subcontractors, or the officers, directors, employees, agents, successors, and assigns of any of them, and the liability of the indemnifying party shall be proportionately reduced.

The foregoing indemnification obligations are conditioned upon the indemnified party promptly notifying the indemnifying party in writing of the claim, suit, or proceeding for which the indemnifying party is obligated under this Subsection, cooperating with, assisting, and providing information to, the indemnifying party as reasonably required, and granting the indemnifying party the exclusive right to defend or settle such claim, suit, or proceeding; provided that any such settlement or compromise includes a release of the indemnified party from all liability arising out of such claim, suit or proceeding.

12. INDEMNIFICATION – INTELLECTUAL PROPERTY The Contractor shall defend, indemnify and hold harmless WSCA-NASPO, the Lead State and Participating Entities along with their officers, agencies, and employees as well as any person or entity for which they may be liable ("Indemnified Party") from and against claims, damages or causes of action including reasonable attorneys' fees and related costs arising out of the claim that the Product or its use, infringes Intellectual Property rights ("Intellectual Property Claim"). The Contractor's obligations under this section shall not extend to any combination of the Product with any other product, system or method, unless:

(1) the Product, system or method is:

(a) provided by the Contractor or the Contractor's subsidiaries or affiliates;

(b) specified by the Contractor to work with the Product; or

(c) reasonably required, in order to use the Product in its intended manner, and the infringement could not have been avoided by substituting another reasonably available product, system or method capable of performing the same function; or

(2) it would be reasonably expected to use the Product in combination with such product, system or method.

The Indemnified Party shall notify the Contractor within a reasonable time after receiving notice of an Intellectual Property Claim. Even if the Indemnified Party fails to provide reasonable notice, the Contractor shall not be relieved from its obligations unless the Contractor can demonstrate that it was prejudiced in defending the Intellectual Property Claim resulting in increased expenses or loss to the Contractor. If the Contractor promptly and reasonably investigates and defends any Intellectual Property Claim, it shall have control over the defense and settlement of it. However, the Indemnified Party must consent in writing for any money damages or obligations for which it may be responsible. The Indemnified Party shall furnish, at the Contractor's reasonable request and expense, information and assistance necessary for such defense. If the Contractor fails to vigorously pursue the defense or settlement of the Intellectual Property Claim, the Indemnified Party may assume the defense or settlement of it and the Contractor shall be liable for all costs and expenses, including reasonable attorneys' fees and related costs, incurred by the Indemnified Party in the pursuit of the Intellectual Property Claim. This section is not subject to any limitations of liability in this Master Agreement or in any other document executed in conjunction with this Master Agreement.

Cisco Response: Cisco respectfully requests replacing this Section with the language from the current Cisco WSCA Data Communications AR-233 contract:

12.1 Contractor will have the obligation and right to defend any claim, action, suit, or proceeding ("IPR Claim") brought against Purchaser so far as it is based on a claim that any product supplied under this Master Agreement infringes Third Party IPR (as defined below). Contractor will indemnify Purchaser against any final judgment entered in respect of such an IPR Claim by a court of competent jurisdiction and against any settlements arising out of such an IPR Claim. Contractor's obligations to defend the IPR Claim and indemnify the Purchaser are conditional upon:

12.1.1 Purchaser notifying Contractor promptly in writing of the IPR Claim or threat thereof;

12.1.2 Purchaser giving Contractor full and exclusive authority for the conduct of the defense and settlement of the IPR Claim and any subsequent appeal; and

12.1.3 Purchaser giving Contractor all information and assistance reasonably requested by Contractor in connection with the conduct of the defense and settlement of the IPR Claim and any subsequent appeal.

12.2 For the purposes of this Master Agreement, "Third Party IPR" means a United States copyright existing as at the date of order or a United States patent issued as at the date of order.

12.3 If an IPR Claim has been made, or in Contractor's reasonable opinion is likely to be commenced, Purchaser agrees to permit Contractor, at its option and expense, either to: (a) procure for Purchaser the right to continue using the product; (b) replace or modify the product so that it becomes non-infringing; or (c) immediately terminate both parties' respective rights and obligations under this Master Agreement with regard to the product, in which case Purchaser will return the product to Contractor and Contractor will refund to Purchaser the price originally paid by Purchaser to Contractor for the product, as depreciated or amortized by an equal annual amount over three (3) years from date of original shipment.

12.4 Notwithstanding the foregoing, Contractor has no liability for, and Purchaser will defend and indemnify Contractor against, any IPR Claim arising from:

12.4.1 the combination, operation, or use of a product supplied under this Master Agreement with any product, device, or software not supplied by Contractor;

12.4.2 the amount or duration of use which Purchaser makes of the product, revenue earned by Purchaser from services it provides which utilize the product, or services offered by Purchaser to external or internal customers;

12.4.3 the alteration or modification of any product supplied under this Master Agreement from and after the date such product is so supplied and such alteration or modification is not made by Contractor;

12.4.4 Contractor's compliance with Purchaser's designs, specifications, or instructions; or

12.4.5 Purchaser's use of the product after Contractor has informed Purchaser of modifications or changes in the product required to avoid such an IPR Claim if the alleged infringement would have been avoided by implementation of Contractor's recommended modifications or changes.

THIS SECTION STATES THE ENTIRE OBLIGATION OF CONTRACTOR AND ITS SUPPLIERS, AND THE EXCLUSIVE REMEDY OF PURCHASER, IN RESPECT OF ANY INFRINGEMENT OR ALLEGED INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHTS OR PROPRIETARY RIGHTS. THIS INDEMNITY OBLIGATION AND REMEDY ARE GIVEN TO PURCHASER SOLELY FOR ITS BENEFIT AND IN LIEU OF, AND CONTRACTOR DISCLAIMS, ALL WARRANTIES, CONDITIONS, AND OTHER TERMS OF NON-INFRINGEMENT WITH RESPECT TO ANY PRODUCT.

13. <u>INDEPENDENT CONTRACTOR</u> The contractor shall be an independent contractor, and as such shall have no authorization, express or implied to bind WSCA-NASPO or the respective states to any agreements, settlements, liability or understanding whatsoever, and agrees not to perform any acts as agent for WSCA-NASPO or the states, except as expressly set forth herein.

Cisco Response: Cisco respectfully requests replacing this Section with the language from the current Cisco WSCA Data Communications AR-233 contract:

Contractor shall be an independent contractor. This Master Agreement does not create any agency, partnership, joint venture, or franchise relationship. No employee of either party shall be or become, or shall be deemed to be or become, an employee of the other party by virtue of the existence or implementation of this Agreement. Each party hereto is an independent contractor. Neither party has the right or authority to, and shall not, assume or create any obligation of any nature whatsoever on behalf of the other party or bind the other party in any respect whatsoever.

14. INDIVIDUAL CUSTOMER Except to the extent modified by a Participating Addendum, each Participating Entity shall follow the terms and conditions of the Master Agreement and applicable Participating Addendum and will have the same rights and responsibilities for their purchases as the Lead State has in the Master Agreement, including but not limited to, any indemnity or to recover any costs allowed in the Master Agreement and applicable Participating Addendum for their purchases. Each Participating Entity will be responsible for its own charges, fees, and liabilities. The Contractor will apply the charges and invoice each Participating Entity individually.

Cisco Response: Agreed.

15. INSURANCE Contractor shall, during the term of this Master Agreement, maintain in full force and effect, the insurance described in this section. Contractor shall acquire such insurance from an insurance carrier or carriers licensed to conduct business in the Participating Entity's state and having a rating of A-, Class VII or better, in the most recently published edition of Best's Reports. Failure to buy and maintain the required insurance may result in this Master Agreement's termination or at a Participating Entity's option, result in termination of its Participating Addendum.

Cisco Response: Agreed.

Coverage shall be written on an occurrence basis. The minimum acceptable limits shall be as indicated below, with no deductible for each of the following categories:

a) Commercial General Liability covering the risks of bodily injury (including death), property damage and personal injury, including coverage for N contractual liability, with a limit of not less than $1 million per occurrence/$2 million general aggregate;

b) Contractor must comply with any applicable State Workers Compensation or Employers Liability Insurance requirements.

Cisco Response: Cisco respectfully requests that the above paragraph be modified as follows**:**

Coverage shall be written on an occurrence basis. The limits shall be as indicated below, with no deductible for each of the following categories:

a) Commercial General Liability covering the risks of bodily injury (including death), property damage, and personal injury, including coverage for contractual liability, with a limit of $1 million per occurrence/$2 million general aggregate;

b) Contractor must comply with any applicable State Workers Compensation or Employers Liability Insurance requirements.

Contractor shall pay premiums on all insurance policies. Such policies shall also reference this Master Agreement and shall have a condition that they not be revoked by the insurer until thirty (30) calendar days after notice of intended revocation thereof shall have been given to Participating Entity by the Contractor.

Cisco Response: Cisco respectfully requests that the second sentence of this Section be deleted.

Prior to commencement of the work, Contractor shall provide to the Participating Entity a written endorsement to the Contractor's general liability insurance policy that (i) names the Participating Entity as an additional insured, (ii) provides that no material alteration, cancellation, non-renewal, or expiration of the coverage contained in such policy shall have effect unless the named Participating Entity has been given at least thirty (30) days prior written notice, and (iii) provides that the Contractor's liability insurance

policy shall be primary, with any liability insurance of the Participating Entity as secondary and noncontributory.

Cisco Response: Cisco respectfully requests that the above paragraph be modified as follows:

Prior to commencement of the work, Contractor shall provide to the Participating Entity a written endorsement to the Contractor's general liability insurance policy that (i) names the Participating Entity as an additional insured, but only to the extent of liabilities falling within Contractor's indemnity obligations pursuant to the terms of this Master Agreement, and (ii) provides that the Contractor's liability insurance policy shall be primary, with any liability insurance of the Participating Entity as secondary and noncontributory.

Contractor shall furnish to Participating Entity copies of certificates of all required insurance within thirty (30) calendar days of the Participating Addendum's effective date and prior to performing any work. Copies of renewal certificates of all required insurance shall be furnished within thirty (30) days after renewal date. These certificates of insurance must expressly indicate compliance with each and every insurance requirement specified in this section. Failure to provide evidence of coverage may, at State's sole option, result in this Master Agreement's termination.

Cisco Response: Cisco respectfully requests that the below be added as the third sentence of the above paragraph.

In addition, should any of the required insurance be cancelled or non-renewed, Contractor shall immediately replace such insurance and provide to Participating Entity a certificate of insurance evidencing the replacement insurance.

Coverage and limits shall not limit Contractor's liability and obligations under this Master Agreement.

Cisco Response: Agreed.

16. <u>LAWS AND REGULATIONS</u> Any and all supplies, services and equipment offered and furnished shall comply fully with all applicable Federal and State laws and regulations.

Cisco Response: Agreed, with the addition of the following language from our existing Cisco WSCA Data Communications AR-233 contract on 1) law changes and 2) Export Restriction. Note that the URL is for customer's ease of reference on individual product export restrictions.

If any law changes after the Effective Date (which such changed law was not reasonably contemplated on the Effective Date) to the material detriment of Contractor (as determined in its sole reasonable discretion), then: (i) the applicable parties may mutually negotiate the up charge to offset the cost of such compliance; (ii) Contractor can unilaterally choose not to ship such product or perform such service (a) under an individual order, or (b) across a like class of all orders under this Master Agreement in consultation with the WSCA Contract Manager, or (c) delete such class of product(s) or service(s) from the scope of this Master Agreement in consultation with the WSCA Contract Manager; or (iii) Contractor may unilaterally terminate the applicable order(s).

***EXPORT RESTRICTIONS**: Notwithstanding anything contained in the Master Agreement to the contrary, the products and technology or direct products thereof (hereafter referred to as "<u>Products and Technology</u>"), supplied by Contractor under this Master Agreement are subject to export controls under the laws and regulations of the United States. Purchaser shall comply with such laws and regulations governing use, export, re-export, and transfer of Cisco Products and Technology and will obtain all required U.S. and local authorizations, permits, or licenses. Cisco, and each participating state and each purchaser each agree to provide the other information, support documents, and assistance, as may reasonably be required by the other, in connection with securing such authorizations or licenses. WSCA's, each Participating State's, and each Purchaser's obligations under this clause shall survive the expiration or termination of the Agreement. Detailed information regarding compliance with U.S. use, export, re-export, and transfer laws may be located at the following URL:* HTTP://WWW.CISCO.COM/WWL/EXPORT/COMPLIANCE_PROVISION.HTML.

17. <u>LICENSE OF PRE-EXISTING INTELLECTUAL PROPERTY</u> Contractor grants to the Participating Entity a nonexclusive, perpetual, royalty-free, irrevocable, unlimited license to publish, translate, reproduce, modify, deliver, perform, display, and dispose of the Intellectual Property, and its derivatives, used or delivered under this Master Agreement, but not created under it ("Pre-existing Intellectual

Property"). The license shall be subject to any third party rights in the Pre-existing Intellectual Property. Contractor shall obtain, at its own expense, on behalf of the Participating Entity, written consent of the owner for the licensed Pre-existing Intellectual Property.

Cisco Response: The only license of Pre-Existing Intellectual Property to be covered in this Contract is Cisco's Software, for which there is an End User License Agreement. Usage rights to any other Pre-Existing Material that would be provided under a Statement of Work would be specifically outlined in the Statement of Work. As such, Cisco requests that this Section be replaced with the Software License section in the current Cisco WSCA Data Communications AR-233 contract below. In addition, please note that certain Cisco technologies have terms that are unique to those technologies. Examples include, but are not limited to, the following: specific usage rights for subscription/term licenses (i.e., IronPort Email and Web Security Offerings, WebEx subscriptions, etc.), limitation or expansion of the number of installation instances (i.e., immersive video conferencing), restricted features, maintenance services included in the cost of the product and limitation on scope of deployment (# of blades). If applicable, such unique terms will be supplied with that particular technology purchase.

17.1 License. Conditioned upon compliance with the terms and conditions of the license granted herein or as represented in Cisco's End User License Agreement, Contractor grants to Customer a nonexclusive and nontransferable license to use for Customer's internal business purposes the Software and the Documentation for which Customer has paid the required license fees.

Customer's license to use the Software shall be limited to, and Customer shall not use the Software in excess of, a single hardware chassis or card or that number of agent(s), concurrent users, sessions, IP addresses, port(s), seat(s), server(s), or site(s), as set forth in the applicable Purchase Order which has been accepted by Contractor and for which Customer has paid to Contractor the required license fee.

Unless otherwise expressly provided in the documentation, Customer shall use the Software solely as embedded in, for execution on, or (where the applicable documentation permits installation on non-Contractor equipment) for communication with Contractor equipment owned or leased by Customer and used for Customer's internal business purposes. For evaluation or beta copies for which Contractor does not charge a license fee, the above requirement to pay license fees does not apply.

17.2 General Limitations. This is a license, not a transfer of title, to the Software and Documentation, and Contractor retains ownership of all copies of the Software and Documentation. Customer acknowledges that the Software and Documentation contain trade secrets of Contractor, its suppliers or licensors, including but not limited to the specific internal design and structure of individual programs and associated interface information. Accordingly, except as otherwise expressly provided under this Agreement, Customer shall have no right, and Customer specifically agrees not to:

17.2.1 transfer, assign or sublicense its license rights to any other person or entity, or use the Software on unauthorized or secondhand Contractor equipment, and Customer acknowledges that any attempted transfer, assignment, sublicense, or use shall be void;

17.2.2 except as approved in writing by Contractor, make error corrections to or otherwise modify or adapt the Software or create derivative works based upon the Software, or permit third parties to do the same;

17.2.3 reverse engineer or decompile, decrypt, disassemble, or otherwise reduce the Software to human-readable form, except to the extent otherwise expressly permitted under applicable law notwithstanding this restriction;

17.2.4 use or permit the software (other than embedded in the product) to be used to perform services for third parties, whether on a service bureau or time sharing basis or otherwise, without the express written authorization of Contractor; or

17.2.5 except and to the extent expressly required by a Participating State's applicable records laws or final court order (provided that the Participating State provides: (1) prior written notice to Contractor of such obligation and (2) the opportunity to oppose such disclosure, provision, or otherwise making available), disclose, provide, or otherwise make available trade secrets contained within the Software and Documentation in any form to any third party without the prior written consent of Contractor. Customer shall implement reasonable security measures to protect such trade secrets.

To the extent required by law, and at Customer's written request, Contractor shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of Contractor's applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Contractor makes such information available.

17.3 Software, upgrades/updates, and additional copies.

NOTWITHSTANDING ANY OTHER PROVISION OF THIS MASTER AGREEMENT: (1) CUSTOMER HAS NO LICENSE OR RIGHT TO USE ANY ADDITIONAL COPIES OR UPGRADES UNLESS CUSTOMER, AT THE TIME OF ACQUIRING SUCH COPY OR UPGRADE, ALREADY HOLDS A VALID LICENSE TO THE ORIGINAL SOFTWARE AND HAS PAID THE APPLICABLE FEE FOR THE UPGRADE OR ADDITIONAL COPIES; (2) USE OF UPGRADES IS LIMITED TO CONTRACTOR EQUIPMENT FOR WHICH CUSTOMER IS THE ORIGINAL END USER PURCHASER OR LESSEE OR WHO OTHERWISE HOLDS A VALID LICENSE TO USE THE SOFTWARE WHICH IS BEING UPGRADED; AND (3) THE MAKING AND USE OF ADDITIONAL COPIES IS LIMITED TO NECESSARY BACKUP PURPOSES ONLY.

17.4 Proprietary Notices. Customer agrees to maintain and reproduce all copyright and other proprietary notices on all copies, in any form, of the Software in the same form and manner that such copyright and other proprietary notices are included on the Software. Except as expressly authorized in this Agreement, Customer shall not make any copies or duplicates of any Software without the prior written permission of Contractor.

17.5 Term and Termination of License. This license granted herein shall remain effective until terminated. Customer may terminate the license at any time by destroying all copies of Software and any Documentation except as to the minimum number of copies required by law to keep for archival records purposes only. Customer's rights under this license will terminate immediately if Customer fails to comply with any material provision of this license and Contractor will give Customer notice of such non-compliance. Upon termination, Customer shall destroy all copies of Software and Documentation in its possession or control.

17.6 Customer Records. Customer grants to Contractor and its independent accountants the right to examine Customer's books, records, and accounts during Customer's normal business hours to verify compliance with this license. In the event such audit discloses non-compliance with this license, Customer shall promptly pay to Contractor the appropriate license fees, plus the reasonable cost of conducting the audit. In all other circumstances, the audit fees shall be paid by Contractor.

18. NO WAIVER OF SOVEREIGN IMMUNITY In no event shall this Master Agreement, any Participating Addendum or any contract or any purchase order issued thereunder, or any act of a Lead State or a Participating Entity, be a waiver by the Participating Entity of any form of defense or immunity, whether sovereign immunity, governmental immunity, immunity based on the Eleventh Amendment to the Constitution of the United States or otherwise, from any claim or from the jurisdiction of any court.

Cisco Response: Agreed.

If a claim must be brought in a federal forum, then it must be brought and adjudicated solely and exclusively within the United States District Court for the Participating State. This section applies to a

claim brought against the Participating State only to the extent Congress has appropriately abrogated the Participating State's sovereign immunity and is not consent by the Participating State to be sued in federal court. This section is also not a waiver by the Participating State of any form of immunity, including but not limited to sovereign immunity and immunity based on the Eleventh Amendment to the Constitution of the United States.

Cisco Response: Agreed.

19. ORDER NUMBERS Master Agreement order and purchase order numbers shall be clearly shown on all acknowledgments, shipping labels, packing slips, invoices, and on all correspondence.

Cisco Response: Agreed. Please also add a Section covering Orders, which appears to be missing from this Agreement. The below is language from our existing WSCA Agreement:

ORDERS. Notwithstanding anything contained in the Master Agreement to the contrary:

1. *Cisco reserves the right to require that purchases be made through Fulfillment Partners. Where so required by Cisco, Purchasers shall not order Products or Services directly from Cisco and shall order same from Fulfillment Partner. Purchaser shall purchase products by issuing a written or electronic Purchase Order, signed or (in the case of electronic transmission) sent by its authorized representative, indicating specific products, quantity, unit price, total purchase price, shipping instructions, requested delivery dates, bill-to and ship-to addresses, tax exempt certifications, if applicable, and any other special instructions.*
2. *Any contingencies on Purchaser's Purchase Orders are not binding upon Contractor. The terms and conditions of this Master Agreement prevail, regardless of any additional or conflicting terms on the Purchase Order, or other correspondence from Purchaser to Contractor and any additional or conflicting terms are deemed rejected by Contractor unless Contractor has expressly agreed to such terms in writing. Mere acceptance or processing of a Purchase Order, Order, or Order Document containing such terms shall not constitute such express consent.*
3. *All Purchase Orders are subject to Contractor's reasonable acceptance (including performing any related credit checks). Contractor shall use commercially reasonable efforts to accept or reject orders in writing within ten (10) days from receipt, or within three (3) business days, if orders are placed electronically.*
4. *Purchaser may defer product shipment up to thirty (30) days from the originally scheduled shipping date, provided written notice is received by Contractor at least ten (10) days before the originally scheduled shipping date. Cancelled orders, rescheduled deliveries, or product configuration changes made by Purchaser less than ten (10) days before the original shipping date are subject to Contractor's acceptance and a charge of fifteen percent (15%) of the total invoice amount relating to the affected Product(s). Contractor reserves the right to reschedule delivery due to configuration changes made within ten (10) days of scheduled shipment. No cancellation shall be accepted by Cisco where products are purchased with implementation services, including but not limited to design, customization, or installation services, except as may be set forth in the agreement or Statement of Work under which the services are to be rendered. Notwithstanding anything to the contrary, if Cisco is delayed in shipping the product for thirty (30) days or more from the original shipping date, the Customer may cancel the order without charge.*
5. *Services. Purchaser may place Purchase Orders for the various services offered by Contractor. The provision of any such services, if accepted by Contractor, shall be subject to the terms and conditions set forth in this Agreement, as well as the then-current terms of service offerings set forth on Contractor's website at http://www.cisco.com/legal/services.html. Contractor reserves the right to subcontract services to a third party maintenance organization to provision services for Purchaser.*
6. *All stated prices are exclusive of any taxes, fees, and duties or other similar amounts, however designated, and including without limitation value added, sales and withholding taxes which are levied or based upon such prices, charges, or upon this Master Agreement. Purchaser will pay sales and use taxes, if any, imposed on the Products and Services acquired under this Master Agreement, or furnish proof of its tax-exempt status upon request. Contractor will pay all other*

taxes based on Contractor's income or gross receipts, or personal property taxes levied or assessed on Contractor's personal property. In the event that the Purchaser is exempt from property and sales taxes, it will not be charged same.

7. *Notwithstanding anything contained in the Master Agreement to the contrary, modifications which Contractor deems necessary to comply with specifications, changed safety standards or governmental regulations, to make the product non-infringing with respect to any patent, copyright, or other proprietary interest, or to otherwise improve the product may be made at any time by Contractor without prior notice to or consent of Purchaser or WSCA, and such altered product shall be deemed fully conforming. Cisco shall employ commercially reasonable efforts to announce, including by electronic posting, product discontinuance or changes other than those set forth in the previous sentence in accordance with Cisco's End-of-Life Policy, which is found at the following URL: http://www.cisco.com/en/us/products/products_end-of-life_policy.html. Purchaser may make a last-time purchase of such products as set forth in such policy.*

20. PARTICIPANTS WSCA-NASPO is the cooperative purchasing arm of the National Association of State Procurement Officials. It is a cooperative group contracting consortium for state government departments, institutions, agencies and political subdivisions (e.g., colleges, school districts, counties, cities, etc.,) for all 50 states, the District of Columbia and the organized US territories. Obligations under this Master Agreement are limited to those Participating States who have signed a Participating Addendum where contemplated by the solicitation. Financial obligations of Participating States are limited to the orders placed by the departments or other state agencies and institutions having available funds. Participating States incur no financial obligations on behalf of political subdivisions. Unless otherwise specified in the solicitation, the resulting award(s) will be permissive.

Cisco Response: Agreed, with the deletion of the fourth sentence.

21. ENTITY PARTICIPATION Use of specific WSCA-NASPO cooperative Master Agreements by state agencies, political subdivisions and other entities (including cooperatives) authorized by individual state's statutes to use state contracts are subject to the approval of the respective State Chief Procurement Official. Issues of interpretation and eligibility for participation are solely within the authority of the respective State Chief Procurement Official.

Cisco Response: Agreed.

22. PAYMENT Payment for completion of a contract order is normally made within 30 days following the date the entire order is delivered or the date a correct invoice is received, whichever is later. After 45 days the Contractor may assess overdue account charges up to a maximum rate of one percent per month on the outstanding balance. Payments will be remitted by mail. Payments may be made via a State or political subdivision "Purchasing Card" with no additional charge.

Cisco Response: Cisco respectfully requests replacement of this Section with the terms in the current Cisco WSCA Data Communications AR-233 contract. In addition, Cisco provided language regarding lease financing which appears to be allowed again according to the Q&A.

Upon and subject to credit approval by Contractor, payment is net thirty (30) days from invoice date and shall be made in U.S. currency. Invoices for products ordered without implementation services shall be rendered by Contractor on or after the date of delivery of such products to the Purchaser. If, at any time, Purchaser is delinquent in payment, or is otherwise in breach of this contract, Contractor may, without prejudice to other rights, withhold shipment (including partial shipments) of any order or require Purchaser to prepay for further shipments. Any sum not paid by Purchaser when due shall bear interest until paid at a rate of 1 percent per month (12 percent per annum) or the maximum legal rate, whichever is less. Purchaser grants Contractor a security interest in products purchased under this contract to secure payment for those products purchased which security interest shall expire upon full payment in accordance with the terms. If requested by Contractor, Purchaser agrees to execute financing statements to perfect this security interest. Payments may be made via a State or political subdivision "Purchasing Card" to Fulfillment Partners under this contract. Acceptance by Purchaser shall be deemed to have occurred upon delivery of the applicable products to the applicable Purchaser. Where permitted by the law of the Participating State/Entity, lease financing is an allowable payment option under the resulting contract. The terms and conditions of the capital

lease financing arrangement with Cisco Capital, or its designated and/or approved financing partner, will be set forth between the purchaser and Cisco Capital or its designated and/or approved financing partner.

23. PUBLIC INFORMATION This Master Agreement and all related documents are subject to disclosure pursuant to the Participating Entity's public information laws.

Cisco Response: Agreed, with the following addition: *"Contractor hereby retains all available rights and remedies under applicable law to protect such information from unauthorized disclosure unless such information is disclosed by the Participating Entity pursuant to statutory requirement or a valid order issued by a court or government agency, and provided that the Participating Entity provides (a) prior written notice to Contractor of such obligation and (b) the opportunity to oppose such disclosure, or such other rights as under law."*

24. RECORDS ADMINISTRATION AND AUDIT The contractor will maintain, or supervise the maintenance of all records necessary to properly account for the payments made to the contractor for costs authorized by this Master Agreement. These records will be retained by the contractor for at least four years after the Master Agreement terminates, or until all audits initiated within the four years have been completed, whichever is later. The contractor agrees to allow WSCA-NASPO, State and Federal auditors, and state agency staff access to all the records of this Master Agreement and any order placed under this Master Agreement, for audit and inspection, and monitoring of services. Such access will be during normal business hours, or by appointment.

Cisco Response: Agreed, with the following changes: 1) Change "supervise" to "require" in the first sentence. 2) Change the last sentence to: "Such access will be 1) with at least fifteen (15) business days advance written notice, 2) during normal business hours, 3) shall not unduly interrupt or interfere with Contractor's normal business operations, and 4) in the event that such audit is conducted by a third party, such third party shall, prior to conducting such audit, execute a confidentiality agreement for the benefit of Contractor in a form reasonably satisfactory to Contractor.

25. REPORTS and ADMINISTRATIVE FEES The contractor shall submit quarterly reports to the WSCA-NASPO Contract Administrator showing the quantities and dollar volume of purchases by each participating entity.

The contractor must pay a WSCA-NASPO administrative fee of one quarter of one percent (.25%) in accordance with the terms and conditions of the Master Agreement. The WSCA-NASPO administrative fee shall be submitted quarterly and is based on sales of products and services. The WSCA-NASPO administration fee is not negotiable. This fee is to be included as part of the pricing submitted with proposal.

Cisco Response: Cisco agrees to submit quarterly sales reports to the WSCA-NASPO Contractor Administrator using the same detailed and comprehensive reporting template that Cisco provides today under its current WSCA Data Communications AR-233 contract. In addition, Cisco agrees to pay the WSCA-NASPO administrative fee of one quarter of one percent (.25%) based on actual sales of all products and services in conjunction with the quarterly usage reports. For purposes of clarification, Cisco understands "sales of products and services" to mean net purchase price, which is Cisco's product list price, minus all applicable contract discounts, rebates, or value added incentives, and excluding sales, use, or other applicable taxes, surcharges, or like fees, to the extent applicable to an order. This definition is consistent with the language in Cisco's current WSCA Data Communications AR-233 contract as set forth in Section D3, Attachment A. Consistent with Cisco's responses to Sections 1.15 and 1.20 in this RFP with respect to the due dates for the quarterly reports and administrative fees, Cisco respectfully requests an exception and proposes to keep the same due dates for both requirements as set forth in Amendment #3 of the current Cisco WSCA Data Communications AR-233 contract, which are as follows:

Quarter #1:	July 1 through September 30, due annually by November 30.
Quarter #2:	October 1 through December 31, due annually by February 28.
Quarter #3:	January 1 through March 31, due annually by May 31.
Quarter #4:	April 1 through June 30, due annually by August 31.

Cisco requests additional time because, as with our current WSCA Data Communications AR-233 contract, we anticipate that we will have another robust list of over 175 subcontractors/resellers from whom to manage and collect reports and administrative fees.

Additionally, some States may require that an additional fee be paid directly to the State on purchases made by procuring entities within that State. For all such requests, the fee level, payment method and schedule for such reports and payments will be incorporated in a Participating Addendum that is made a part of the Master Agreement. The contractor may adjust the Master Agreement pricing accordingly for purchases made by procuring agencies within the jurisdiction of the State. All such agreements may not affect the WSCA-NASPO administrative fee or the prices paid by the procuring agencies outside the jurisdiction of the State requesting the additional fee.

Cisco Response: Agreed.

26. STANDARD OF PERFORMANCE AND ACCEPTANCE The Standard of Performance applies to all Product(s) purchased under this Master Agreement, including any additional, replacement, or substitute Product(s) and any Product(s) which are modified by or with the written approval of Contractor after Acceptance by the Participating Entity. The Acceptance Testing period shall be thirty (30) calendar days or other time period identified in the solicitation or the Participating Addendum, starting from the day after the Product is installed and Contractor certifies that the Product is ready for Acceptance Testing. If the Product does not meet the Standard of Performance during the initial period of Acceptance Testing, Participating Entity may, at its discretion, continue Acceptance Testing on a day-to-day basis until the Standard of Performance is met. Upon rejection, the Contractor will have fifteen (15) calendar days to cure the Standard of Performance issue(s). If after the cure period, the Product still has not met the Standard of Performance Participating Entity may, at its option: (1) declare Contractor to be in breach and terminate the Order; (2) demand replacement Product from Contractor at no additional cost to Participating Entity; or, (3) continue the cure period for an additional time period agreed upon by the Participating Entity and the Contractor. Contractor shall pay all costs related to the preparation and shipping of Product returned pursuant to the section. No Product shall be accepted and no charges shall be paid until the Standard of Performance is met. The warranty period will begin upon Acceptance.

Cisco Response: Section 8, which contains proposed language from our existing Cisco WSCA Data Communications AR-233 contract, covers acceptance terms, return rights, and warranty references. As such, Cisco respectfully requests deletion of this Section**.**

27. SYSTEM FAILURE OR DAMAGE In the event of system failure or damage caused by the Contractor or its Product, the Contractor agrees to use its best efforts to restore or assist in restoring the system to operational capacity.

Cisco Response: Cisco respectfully requests deletion of this Section. Our warranty and product maintenance provisions would cover the services provided. If additional work is needed above these provisions, then this would be on a paid basis.

28. TITLE OF PRODUCT Upon Acceptance by the Participating Entity, Contractor shall convey to Participating Entity title to the Product free and clear of all liens, encumbrances, or other security interests.Transfer of title to the Product shall include an irrevocable and perpetual license to use the Embedded Software in the Product. If Participating Entity subsequently transfers title of the Product to another entity, Participating Entity shall have the right to transfer the license to use the Embedded Software with the transfer of Product title. A subsequent transfer of this software license shall be at no additional cost or charge to either Participating Entity or Participating Entity's transferee.

Cisco Response: Cisco requests that it be clarified that Title and Risk of Loss transfers at delivery of the product. This is consistent with our current Cisco WSCA Data Communications AR-233 contract. Also, 1) Cisco has a Transfer Policy that differs with this Section, 2) certain products may not have a perpetual license and any such terms will be per our End User License Agreement (EULA). As such, please replace this Section with the following:

> *Acceptance by Purchaser shall be deemed to have occurred upon delivery of the applicable products to the applicable Purchaser. Title and risk of loss shall pass to Purchaser upon delivery. Any transfers of Embedded Software shall be per Contractor's then-current Transfer and Re-Licensing Policy.*

29. WAIVER OF BREACH Failure of Lead State or Participating Entity to declare a default or enforce any rights and remedies shall not operate as a waiver under this Master Agreement or Participating Addendum. Any waiver by the Lead State or Participating Entity must be in writing. Waiver by the Lead State or Participating Entity of any default, right or remedy under this Master Agreement or Participating Addendum, or breach of any terms or requirements shall not be construed or operate as a waiver of any subsequent default or breach of such term or requirement, or of any other term or requirement under this Master Agreement or Participating Addendum.

Cisco Response: Agreed, with the change that "or Contractor" be added in each instance of "Lead State or Participating Entity."

30. WARRANTY The Contractor warrants for a period of one year from the date of Acceptance that: (a) the Product performs according to all specific claims that the Contractor made in its response to the solicitation, (b) the Product is suitable for the ordinary purposes for which such Product is used, (c) the Product is suitable for any special purposes identified in the solicitation or for which the Participating Entity has relied on the Contractor's skill or judgment, (d) the Product is designed and manufactured in a commercially reasonable manner, and (e) the Product is free of defects. Upon breach of the warranty, the Contractor will repair or replace (at no charge to the Participating Entity) the Product whose nonconformance is discovered and made known to the Contractor. If the repaired and/or replaced Product proves to be inadequate, or fails of its essential purpose, the Contractor will refund the full amount of any payments that have been made. The rights and remedies of the parties under this warranty are in addition to any other rights and remedies of the parties provided by law or equity, including, without limitation, actual damages, and, as applicable and awarded under the law, to a prevailing party, reasonable attorneys' fees and costs.

Cisco Response: Cisco respectfully requests replacing this Section with the language from the current Cisco WSCA Data Communications AR-233 contract.

30. All products are sold with Contractor's standard limited warranty listed below:

30.1 Hardware. Contractor warrants that from the date of shipment by Contractor to Customer, and continuing for a period of the longer of (a) ninety (90) days or (b) the period set forth in the Warranty Card accompanying the product, the Hardware will be free from defects in material and workmanship, under normal use. This limited warranty extends only to the original user of the product. Customer's sole and exclusive remedy and the entire liability of Contractor and its suppliers under this limited warranty will be, at Contractor's or its service center's option, shipment of a replacement within the period and according to the replacement process described in the Warranty Card, or a refund of the purchase price, if the Hardware is returned to the party supplying it to Customer, if different than Contractor, freight and insurance prepaid. Contractor replacement parts, used in Hardware repair, may be new or equivalent to new. Contractor's obligations hereunder are conditioned upon the return of affected products, in accordance with Contractor's then-current Return Material Authorization (RMA) procedures.

30.2 Software. Contractor warrants that from the date of delivery by Contractor to Customer (but in case of resale by a Contractor reseller, commencing not more than ninety (90) days after original shipment by Contractor), and continuing for a period of the longer of (a) ninety (90) days or (b) the period set forth in the Warranty Card accompanying the product (if any): (a) the media on which the Software is furnished will be free of defects in materials and workmanship, under normal use; and (b) the Software substantially conforms to its published specifications. The date of shipment of a product by Contractor is set forth on the packaging material in which the product is shipped. Except for the foregoing, the Software is provided AS IS. This limited warranty extends only to the Customer who is the original licensee. Customer's sole and exclusive remedy and the entire liability of Contractor and its suppliers under this limited warranty will be, at Contractor or its service center's option, repair, replacement, or refund of the Software if reported (or, upon request, returned) to the party supplying the Software to Customer, if different than Contractor. In no event does Contractor warrant that the Software is error free or that Customer will be able to operate the Software without problems or interruptions. In addition, due to the continual development of new techniques for intruding upon and attacking networks, Contractor does not warrant that the Software or any equipment,

system, or network on which the Software is used will be free of vulnerability to intrusion or attack.

30.3 Restrictions. This warranty does not apply if the product (a) has been altered, except by Contractor, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Contractor, (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident; or (d) is sold or, in the case of Software, licensed, for beta, evaluation, testing, or demonstration purposes for which Contractor does not receive a payment of purchase price or license fee.

30.4 DISCLAIMER OF WARRANTY. EXCEPT AS SPECIFIED IN THIS WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, SATISFACTORY QUALITY, OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE WARRANTY PERIOD. This disclaimer shall apply even if the above-stated warranty fails of its essential purpose.

The above warranty DOES NOT apply to any beta software, any software made available for testing or demonstration purposes, any temporary software modules or any software for which Contractor does not receive a license fee. All such software is provided AS IS without any warranty whatsoever.

31. <u>ASSIGNMENT OF ANTITRUST RIGHTS</u> Contractor irrevocably assigns to a Participating Entity any claim for relief or cause of action which the Contractor now has or which may accrue to the Contractor in the future by reason of any violation of state or federal antitrust laws (15 U.S.C. § 1-15 or a Participating Entity's state antitrust provisions), as now in effect and as may be amended from time to time, in connection with any goods or services provided to the Contractor for the purpose of carrying out the Contractor's obligations under this Master Agreement or Participating Addendum, including, at a Participating Entity's option, the right to control any such litigation on such claim for relief or cause of action.

Cisco Response: Cisco respectfully takes exception to this Section and requests its deletion. Upon discussion of the concern and the intent behind the language, we may consider a mutually agreeable version of this Section.

Contractor shall require any subcontractors hired to perform any of Contractor's obligations, under this Master Agreement or Participating Addendum, to irrevocably assign to a Participating Entity, as third party beneficiary, any right, title or interest that has accrued or which may accrue in the future by reason of any violation of state or federal antitrust laws (15 U.S.C. § 1-15 or a Participating Entity's state antitrust provisions), as now in effect and as may be amended from time to time, in connection with any goods or services provided to the subcontractor for the purpose of carrying out the subcontractor's obligations to the Contractor in pursuance of this Master Agreement or Participating Addendum, including, at a Participating Entity's option, the right to control any such litigation on such claim for relief or cause of action.

Cisco Response: Cisco respectfully takes exception to this Section and requests its deletion. Upon discussion of the concern and the intent behind the language, we may consider a mutually agreeable version of this Section.

32. <u>WSCA-NASPO eMARKET CENTER</u> Awarded responders are required to participate in the WSCA-NASPO eMarket Center and, working through WSCA-NASPO's contractor (SciQuest), connect with the eMarket Center. The ideal situation would be to use either a hosted (by SciQuest) or Punchout Level 2 catalog configurations, but actual requirements will be determined by the Lead State Contract Administrator, WSCA-NASPO, WSCA-NASPO's contractor (SciQuest) and the awarded contractor, after award. Participation does not require an awarded responder to have any special level of technology or technological understanding.

Cisco Response: Agreed.

Definitions

Acceptance - means a written notice from a purchasing entity to contractor advising Contractor that the Product has passed its Acceptance Testing. Acceptance of a product for which acceptance testing is not required shall occur following the completion of delivery, installation, if required, and a reasonable time for inspection of the product, unless the Purchasing Entity provides a written notice of rejection to contractor.

Acceptance Testing - means the process for ascertaining that the Product meets the standards set forth in the section titled Standard of Performance and Acceptance, prior to Acceptance by the Purchasing Entity.

Cisco Response: Cisco requests deletion of this definition as it is no longer used.

Contractor - means the person or entity delivering Products or performing services under the terms and conditions set forth in this Master Agreement.

Cisco Response: Cisco requests the addition of that following at the end of this definition: *"…., including Contractor's Fulfillment Partners."*

Intellectual Property – means any and all patents, copyrights, service marks, trademarks, trade secrets, trade names, patentable inventions, or other similar proprietary rights, in tangible or intangible form, and all rights, title, and interest therein.

Cisco Response: Cisco requests deletion of this definition as it is no longer used. Third-party IPR is used in its place and is defined within the agreement.

Lead State - means the State conducting this cooperative solicitation and centrally administering any resulting Master Agreement with the permission of the Signatory States.

Master Agreement – means the underlying agreement executed by and between the Lead State, as WSCA-NASPO contract administrator, acting on behalf of WSCA-NASPO, and the Contractor, as now or hereafter amended.

Order - means any purchase order, sales order, or other document used by a Participating Entity to order the Products.

Participating Addendum - means a bilateral agreement executed by a Contractor and a Participating Entity incorporating this Master Agreement and any other additional Participating Entity specific language or other requirements ,e.g. ordering procedures specific to the Participating Entity, other terms and conditions.

Participating Entity - means a state, or other legal entity, properly authorized by a state to enter into the Master Agreement or Participating Addendum or who is authorized to order under the Master Agreement or Participating Addendum.

Product - Any equipment, software (including embedded software), documentation, or deliverable supplied or created by the Contractor pursuant to this Master Agreement.

Cisco Response: Agreed, with the addition that any software provided under the Master Agreement shall be governed by the terms herein and the Contractor's End User License Agreement included in the Additional Terms and Conditions.

Please note that Demo Loan Equipment and Try and Buy are addressed in our Cisco WSCA Data Communications AR-233 contract. We do not believe these terms need to be addressed in this new Master Agreement; however, please let us know if you have any concerns.

WSCA-NASPO -is a cooperative group contracting consortium for state procurement officials, representing departments, institutions, agencies, and political subdivisions (i.e., colleges, school districts, counties, cities, etc.) for all states and the District of Columbia. WSCA-NASPO is a cooperative purchasing arm of the National Association of State Procurement Officials (NASPO).

Additional Definitions and Alternative Terms for Consideration

Below are additional definitions and alternative terms for consideration by the sourcing teams depending upon the nature of the solicitation and negotiations between the Contractor and Vendor.

Embedded Software - means one or more software applications which permanently reside on a computing device.

Machine Code – means microcode, basic input/output system code, utility programs, device drivers, diagnostics, and another code delivered with a computing device for the purpose of enabling the function of the computing device, as stated in its published specifications.

Cisco Response: Cisco does not believe that the above two definitions are necessary for our product terms. We look forward to discussing the applicability of these definitions as well as the need to add any additional definitions based on our discussions.

Please add the following definitions:

Customer - *see "Purchaser" or "Participating Entity."*

Documentation *– means user manuals, training materials, product descriptions and specifications, technical manuals, license agreements, supporting materials, and other information relating to Products or Advanced Services offered by Contractor, whether distributed in print, electronic, CD-ROM, or video format.*

Fulfillment Partner *(also referred to as "Reseller" or "Authorized Reseller") - means a third-party contractor qualified and authorized by Contractor, and approved by the Participating State under a Participating Addendum, who may, to the extent authorized by Contractor, fulfill any of the requirements of this Master Agreement including but not limited to providing Products and Services under this Master Agreement and billing Purchasers directly for such Products and Services. Contractor may, upon written notice to the Participating State, add or delete authorized Fulfillment Partners as necessary at any time during the contract term. Fulfillment Partner has no authority to amend this Master Agreement or to bind Contractor to any additional terms and conditions.*

Participating State *– see "Participating Entity."*

Purchaser *- (also referred to as "Customer") means: (a) the Lead State, (b) any office, department, commission, council, board, committee, institution, legislative body, agency, public authority, public benefit corporation, other government corporation, or public educational institution of a Participating State or a Local Public Body within such Participating State, provided that such entity is authorized, under applicable laws, rules and/or regulations of the Participating State, (i) to purchase Product(s) and Services pursuant to this Master Agreement solely by execution of the applicable Participating Addendum, and (ii) to legally bind such body to the terms of such agreement solely by the issuance of a Purchase Order, Order, or Order Document in accordance with and pursuant to this Master Agreement, and (iii) has been authorized by the WSCA Contract Manager and Contractor to participate under this Master Agreement.*

Purchase Order – see "Order."

Services - "Services" means those services within the scope of this Master Agreement, and listed on Contractor's then-current Global Price List, including consulting, training, installation and maintenance services, and/or other services related to the products being acquired and further described at cisco.com and which are subject to the terms of service set forth in the SOW Terms and Conditions.

(Revised March 2013)

Appendix B —
State of Utah Standard Information Technology Terms and Conditions with Noted Exceptions
(For WSCA Contracts and DTS Related Contracts)

Cisco Response: Cisco and WSCA have operated successfully with the current terms and conditions for over the last 5 years. As such, we recommend in certain sections that we utilize the terms of our existing agreement. These terms have served all parties well, including the Participating States, which serves as a testament to the robust and comprehensive nature of the existing agreement. This approach will also serve to expedite reaching final agreement on terms and conditions.

Cisco's understanding is that these State of Utah Standard Information Technology Terms and Conditions represent the State of Utah Participating Addendum and these would take priority over the Master Agreement Terms and Conditions with respect to purchases made by a State of Utah entity.

1. **AUTHORITY:** Provisions of this contract are pursuant to the authority set forth in 63G-6, Utah Code Annotated, 1953, as amended, Utah State Procurement Rules (Utah Administrative Code Section R33), and related statutes which permit the State to purchase certain specified services, and other approved purchases for the State.

Cisco Response: Agreed

2. **CONTRACT JURISDICTION, CHOICE OF LAW, AND VENUE:** The provisions of this contract shall be governed by the laws of the State of Utah. The parties will submit to the jurisdiction of the courts of the State of Utah for any dispute arising out of this Contract or the breach thereof. Venue shall be in Salt Lake City, in the Third Judicial District Court for Salt Lake County.

Cisco Response: Agreed

3. **LAWS AND REGULATIONS:** The Contractor and any and all supplies, services, equipment, and construction furnished under this contract will comply fully with all applicable Federal and State laws and regulations, including applicable licensure and certification requirements.

Cisco Response: Agreed

4. **RECORDS ADMINISTRATION:** The Contractor shall maintain, or supervise the maintenance of all records necessary to properly account for the payments made to the Contractor for costs authorized by this contract. These records shall be retained by the Contractor for at least four years after the contract terminates, or until all audits initiated within the four years, have been completed, whichever is later. The Contractor agrees to allow State and Federal auditors, and State Agency Staff, access to all the records to this contract, for audit and inspection, and monitoring of services. Such access will be during normal business hours, or by appointment.

Cisco Response: Agreed, with the clarification that any such access shall 1) be limited to once per year 2) be with at least fifteen (15) business days advance written notice, 3) be during normal business hours, 4) not unduly interrupt or interfere with Contractor's normal business operations, and 4) in the event that such audit is conducted by a third party, such third party shall, prior to conducting such audit, execute a confidentiality agreement for the benefit of Contractor in a form reasonably satisfactory to Contractor. Please note that this is also in the WSCA-NASPO Master Agreement Terms and Conditions in Section 24. As such, please consider deleting this Section due to redundancy.

5. **CERTIFY REGISTRATION AND USE OF EMPLOYMENT "STATUS VERIFICATION SYSTEM":** The Status Verification System, also referred to as "E-verify", only applies to contracts issued through a Request for Proposal process, and to sole sources that are included within a Request for Proposal. It does not apply to Invitation for Bids or to the Multi-Step Process.

   1. **Status Verification System**

      (1) Each offeror and each person signing on behalf of any offeror certifies as to its own entity, under penalty of perjury, that the named Contractor has registered and is participating in the Status Verification System to verify the work eligibility status of the contractor's new employees that are

employed in the State of Utah in accordance with applicable immigration laws including UCA Section 63G-12-302.

(2) The Contractor shall require that the following provision be placed in each subcontract at every tier: "The subcontractor shall certify to the main (prime or general) contractor by affidavit that the subcontractor has verified through the Status Verification System the employment status of each new employee of the respective subcontractor, all in accordance with applicable immigration laws including UCA Section 63G-12-302 and to comply with all applicable employee status verification laws. Such affidavit must be provided prior to the notice to proceed for the subcontractor to perform the work."

(3) The State will not consider a proposal for award, nor will it make any award where there has not been compliance with this Section.

(4) Manually or electronically signing the Proposal is deemed the Contractor's certification of compliance with all provisions of this employment status verification certification required by all applicable status verification laws including UCA Section 63G-12-302.

Cisco Response: Agreed

2 Indemnity Clause for Status Verification System

(1) Contractor (includes, but is not limited to any Contractor, Design Professional, Designer or Consultant) shall protect, indemnify and hold harmless, the State and its officers, employees, agents, representatives and anyone that the State may be liable for, against any claim, damages or liability arising out of or resulting from violations of the above Status Verification System Section whether violated by employees, agents, or contractors of the following: (a) Contractor; (b) Subcontractor at any tier; and/or (c) any entity or person for whom the Contractor or Subcontractor may be liable.

(2) Notwithstanding Section 1. above, Design Professionals or Designers under direct contract with the State shall only be required to indemnify the State for a liability claim that arises out of the design professional's services, unless the liability claim arises from the Design Professional's negligent act, wrongful act, error or omission, or other liability imposed by law except that the design professional shall be required to indemnify the State in regard to subcontractors or subconsultants at any tier that are under the direct or indirect control or responsibility of the Design Professional, and includes all independent contractors, agents, employees or anyone else for whom the Design Professional may be liable at any tier.

Cisco Response: Cisco respectfully requests deletion of this Section. Liability for breach of the contract and indemnification are covered in the WSCA-NASPO Master Agreement Terms and Conditions and elsewhere in this Agreement. In addition, subsection (2) does not apply to the scope of this contract.

6. CONFLICT OF INTEREST: Contractor represents that none of its officers or employees are officers or employees of the State of Utah, unless disclosure has been made in accordance with 67-16-8, Utah Code Annotated, 1953, as amended.

Cisco Response: Agreed

7. CONFLICT OF INTEREST WITH STATE EMPLOYEES: In addition to the provisions of State of Utah Terms and Conditions # 6, Conflict of Interest, the Contractor certifies that no person in the State's employment, directly or through subcontract, will receive any private financial interest, direct or indirect, in the contract. The Contractor will not hire or subcontract with any person having such conflicting interest.

***Cisco Response**:* Agreed, with the understanding that the last sentence will be replaced with the following: "*The Contractor ensures that its employees will comply with Contractor's Conflict of Interest policy.*"

8. CONTRACTOR ACCESS TO SECURE STATE FACILITIES / CRIMINAL CONVICTION INFORMATION / FORMER FELONS: The Contractor shall provide (at its own expense) the State with sufficient personal information about its agents or employees, and the agents and employees of its subcontractors (if any) who will enter upon secure premises controlled, held, leased, or occupied by the State during the course of performing this contract so as to facilitate a criminal record check, at State expense. "Sufficient personal information" about its agents or employees, and the agents and

employees of its subcontractors (if any) means for the Contractor to provide to the State Project Manager, in advance of any on-site work, a list of the full names of the designated employees, including their social security number, driver license number and the state of issuance, and their birth date. Thereafter, on their first site visit, each contractor employee expected to work on-site shall be fingerprinted by the State, and the State is authorized to conduct a federal criminal background check based upon those fingerprints and personal information provided. Contractor, in executing any duty or exercising any right under this contract, shall not cause or permit any of its agents or employees, and the agents and employees of its subcontractors (if any) who have been convicted of a felony and misdemeanors other than minor misdemeanors to enter upon any premises controlled, held, leased, or occupied by the State. A felony and misdemeanor are defined by the jurisdiction of the State of Utah, regardless of where the conviction occurred.

Cisco Response: Cisco respectfully requests that this section be reworded as follows:

"The Contractor shall provide (at its own expense) the State with sufficient personal information about its agents or employees, and the agents and employees of its subcontractors (if any) who will enter upon secure premises controlled, held, leased, or occupied by the State during the course of performing this contract so as to facilitate a criminal record check upon receiving the individuals' consent in accordance with applicable law, at State expense. "Sufficient personal information" about its agents or employees, and the agents and employees of its subcontractors (if any) means for the Contractor to provide to the State Project Manager, in advance of any onsite work, a list of the full names of the designated employees. Contractor, in executing any duty or exercising any right under this contract, shall not knowingly cause or permit any of its agents or employees, and the agents and employees of its subcontractors (if any) who have been convicted of a felony and misdemeanors other than minor misdemeanors to enter upon any premises controlled, held, leased, or occupied by the State. A felony and misdemeanor are defined by the jurisdiction of the State of Utah, regardless of where the conviction occurred."

9. **DRUG-FREE WORKPLACE:** The Contractor agrees to abide by the Department of Technology Services (DTS) drug-free workplace policies while on State of Utah premises. DTS will provide the Contractor with a copy of these written "drug-free workplace policies" upon request.

Cisco Response: Cisco requests provision of the "Drug-Free Workplace Policies" before full agreement to this Section.

10. **CODE OF CONDUCT:** When Contractor employees are working on-site, the Contractor agrees to follow and enforce DTS Policy 2000-001 Code of Conduct. If Contractor is working at facilities controlled by other State agencies, Contractor agrees to follow and enforce the Code of Conduct Policy of these other State agencies when Contractor is providing services at these facilities under provisions of this contract. The Contractor will assure that each employee or volunteer under Contractor's supervision receives a copy of such Code of Conduct, and a signed statement to this effect must be in each Contractor or Subcontractor employee's/volunteer's file and is subject to inspection and review by the State's monitors. Upon request, DTS agrees to provide Contractor with a copy of any applicable codes of conduct. If a Contractor or Subcontractor is working at any State agency which has a Code of Conduct applicable to this Contract, the DTS Project Manager will provide the Contractor with a copy in advance of the Contractor's on-site contract services performance.

Cisco Response: Agreed, with a change of the first and third sentences, respectively, to the following. (Cisco's Code of Conduct is available on line and will be provided to the State as necessary.)

First sentence replacement: "*When Contractor employees are working onsite, the Contractor agrees to follow and enforce DTS Policy 2000-001 Code of Conduct or Contractor's Code of Conduct ("Code of Conduct")."*

Third sentence replacement: *"The Contractor will assure that each employee under Contractor's supervision receives a copy of such Code of Conduct."*

11. **INDEMNITY CLAUSE:** The Contractor agrees to indemnify, save harmless, and release the State of Utah, and all its officers, agents, volunteers, and employees from and against any and all loss, damages, injury, liability, suits, and proceedings arising out of the performance of this contract which are caused in whole or in part by the acts or negligence of the Contractor's officers, agents, volunteers, or employees, but not for claims arising from the State's sole negligence. The parties agree that if there are any Limitations of the Contractor's Liability, including a limitation of liability for anyone for whom the

Contractor is responsible, such Limitations of Liability will not apply to injuries to persons, including death, or to damages to property.

Cisco Response: Cisco respectfully requests replacing this Section with language from the current Cisco WSCA Data Communications AR-233. This language (modified slightly to fit terminology of this contract) is:

"Each party to this Agreement shall defend, indemnify, and hold harmless the other, its corporate affiliates and their respective officers, directors, employees, and agents and their respective successors and assigns from and against any and all claims, losses, liabilities, damages, and expenses (including, without limitation, reasonable attorneys' fees), including without limitation those based on contract or tort, arising out of or in connection with a claim, suit, or proceeding brought by a third party based upon bodily injury (including death) or damage to tangible personal property (not including lost or damaged data) arising from the negligent or intentional acts or omissions of the indemnifying party or its subcontractors, or the officers, directors, employees, agents, successors and assigns of any of them. In the event that the indemnified party's or a third party's negligent or intentional acts or omissions contributed to cause the injury or damage for which a claim of indemnity is being asserted against the indemnifying party hereunder, the damages and expenses (including, without limitation, reasonable attorneys' fees) shall be allocated or reallocated, as the case may be, between the indemnified party, the indemnifying party, and any other party bearing responsibility in such proportion as appropriately reflects the relative fault of such parties, or their subcontractors, or the officers, directors, employees, agents, successors, and assigns of any of them, and the liability of the indemnifying party shall be proportionately reduced.

The foregoing indemnification obligations are conditioned upon the indemnified party promptly notifying the indemnifying party in writing of the claim, suit, or proceeding for which the indemnifying party is obligated under this Subsection, cooperating with, assisting, and providing information to, the indemnifying party as reasonably required, and granting the indemnifying party the exclusive right to defend or settle such claim, suit, or proceeding; provided that any such settlement or compromise includes a release of the indemnified party from all liability arising out of such claim, suit or proceeding."

12. **EMPLOYMENT PRACTICES CLAUSE:** The Contractor agrees to abide by the provisions of Title VI and VII of the Civil Rights Act of 1964 (42USC 2000e) which prohibits discrimination against any employee or applicant for employment or any applicant or recipient of services, on the basis of race, religion, color, or national origin; and further agrees to abide by Executive Order No. 11246, as amended, which prohibits discrimination on the basis of sex; 45 CFR 90 which prohibits discrimination on the basis of age; and Section 504 of the Rehabilitation Act of 1973, or the Americans with Disabilities Act of 1990 which prohibits discrimination on the basis of disabilities. Also, the Contractor agrees to abide by Utah's Executive Order, dated March 17, 1993, which prohibits sexual harassment in the work place.

Cisco Response: Agreed

13. **TERMINATION:** Unless otherwise stated in the Special Terms and Conditions, this contract may be terminated, with cause by either party, in advance of the specified termination date, upon written notice being given by the other party. The party in violation will be given ten (10) working days after notification to correct and cease the violations, after which the contract may be terminated for cause. This contract may be terminated without cause, in advance of the specified expiration date, by either party, upon sixty (60) days prior written notice being given the other party. On termination of this contract, all accounts and payments will be processed according to the financial arrangements set forth herein for approved services rendered to date of termination.

    In the event of such termination, and professional services apply to the contract; the Contractor shall be compensated for services properly performed under this Contract up to the effective date of the notice of termination. The Contractor agrees that in the event of such termination for cause or without cause, Contractor's sole remedy and monetary recovery from the State is limited to full payment for all work properly performed as authorized under this Contract up to the date of termination as well as any reasonable monies owed as a result of the Contractor having to terminate contracts necessarily and appropriately entered into by the Contractor pursuant to this Contract. Contractor further acknowledges that in the event of such termination, all work product, which includes but is not limited to all manuals, forms, contracts, schedules, reports, and any and all documents produced by Contractor under this Contract up to the date of termination are the property of the State and shall be promptly delivered to the State.

Cisco Response: Per our understanding of the Q&A prior to contract submission, it appears that the "Special Terms and Conditions" are this document. If this understanding is correct, please delete "Unless otherwise stated in the Special Terms and Conditions."

Please change the second sentence to the following: *"Such termination shall be effective a) immediately upon providing written notice to the breaching party if the breach is not capable of being cured, or (b) sixty (60) calendar days after providing written notice to the breaching party if the breaching party otherwise fails to cure a material breach within such sixty (60) calendar day period, or commence cure within such sixty (60) calendar day period, or diligently pursue completion of such cure."*

Please change the last sentence of first paragraph of this Section to*: "On termination of this contract, all accounts and payments will be processed according to the financial arrangements set forth herein for products delivered and/or approved services rendered to date of termination."*

Please delete the last sentence of second paragraph of this Section. Ownership of Work Product will be covered, as applicable, in the Master Services Agreement.

Please add the following from the current Cisco WSCA Data Communications AR-233:

"Rights upon Termination or Expiration.

1. *Upon termination or expiration of this contract, (a) Contractor reserves the right to cease all further delivery of product or services, (b) all outstanding invoices become due and payable within thirty (30) days of termination, and (c) all rights and licenses of State under this contract shall terminate. If Contractor agrees to complete delivery of any further products or services due against any existing accepted Purchase Orders, then State shall pay for such products or services in advance within thirty (30) days.*
2. *Except for a termination of this contract resulting from State's breach of Contractor's proprietary rights and software licensing, Confidential Information, or Export, Re-Export, Transfer & Use Controls, upon termination or expiration of this contract, State may continue to use, in accordance with the terms and conditions of this contract, products provided to it by Contractor prior to the date of termination or expiration, provided payment has been made in full for such products.*
3. *Upon termination or expiration of this contract, State shall immediately return to Contractor all Confidential Information (including all copies thereof) then in State's possession, custody, or control (except that State may retain one archival copy for records retention purposes only as required by law); provided that, except for a termination resulting from State's breach of proprietary rights and software licensing, Confidential Information, or Export Restrictions, State may retain a sufficient amount of such Confidential Information and material to operate its installed base of products.*
4. *In the event of any termination pursuant to this Section, and unless otherwise required by law or court of competent jurisdiction, State shall remain obligated to comply in perpetuity with the provisions of Contractor's Software License terms, Export Restrictions, and Confidential Information for purchased product."*

14. SUSPENSION OF WORK: Should circumstances arise which would cause the State to suspend the work, but not terminate the contract, this will be done by formal notice. The work may be reinstated upon advance formal notice from the State.

Cisco Response: Agreed, with clarification that State will reimburse Contractor for products delivered or services performed through the date of suspension of work.

15. NONAPPROPRIATION OF FUNDS: The Contractor acknowledges that the State cannot contract for the payment of funds not yet appropriated by the Utah State Legislature. If funding to the State is reduced due to an order by the Legislature or the Governor, or is required by State law, or if federal funding (when applicable) is not provided, the State may terminate this contract or proportionately reduce the services and purchase obligations and the amount due from the State upon 30 days written notice. In the case that funds are not appropriated or are reduced, the State will reimburse Contractor for products delivered or services performed through the date of cancellation or reduction, and the State will not be liable for any future commitments, penalties, or liquidated damages.

Cisco Response: Cisco respectfully asks that this Section be deleted and be replaced with the following from both the current Cisco WSCA Data Communications AR-233 and the agreement that was assigned to Cisco from Tandberg:

"State shall have no liability to Contractor beyond funds that are appropriated and made available to the State by the applicable legislative body.

If sufficient funds are not appropriated by legislative action to a State as to any future period, State may terminate its Order(s) prospectively as to such future performance impacted by and to the extent of non-appropriation, or otherwise work with Contractor to arrive at a mutually acceptable resolution of the situation. State shall notify Contractor in writing of such non-appropriation with thirty (30) calendar days' written notice. If funding to the State is reduced due to an order by the Legislature or the Governor, or is required by State law, or if federal funding (when applicable) is not provided, the State may terminate this contract upon 30 days written notice.

No penalty shall accrue to States in the event this section shall be exercised. This section shall not be construed to permit a State to terminate its Order(s) as to the period for which appropriations were made and available or to permit State to terminate this agreement in order to acquire similar Products or Services from a third party.

Any cancellation under this provision shall not affect the rights and obligations of either party attending orders outstanding up to the time of non-appropriation of funds, e.g., any right of State to indemnification by the Contractor, rights of payment for goods/services delivered and accepted, and rights attending any warranty or default in performance in association with any prior order."

16. **SALES TAX EXEMPTION:** The State of Utah's sales and use tax exemption number is 11736850-010-STC, located at http://purchasing.utah.gov/contract/documents/salestaxexemptionformsigned.pdf. The tangible personal property or services being purchased are being paid from State funds and used in the exercise of that entity's essential functions. If the items being purchased are construction materials, they will be converted into real property by employees of this government entity, unless otherwise stated in the contract.

Cisco Response: Agreed

17. **SECURE PROTECTION AND HANDLING OF DATA:**

Cisco Response: We look forward to discussing with the State the applicability of this Section to the products and services Cisco will provide under the award. Once we have these discussions, we will be better able to provide complete comments. The below represents initial concerns.

1. **Network Security**: Contractor agrees at all times to maintain network security that - at a minimum - includes: network firewall provisioning, intrusion detection, and regular third party penetration testing. Likewise Contractor agrees to maintain network security that conforms to one of the following:
    a. Those standards the State of Utah applies to its own network, found at http://www.dts.utah.gov;
    b. Current standards set forth and maintained by the National Institute of Standards and Technology, includes those at: HTTP://WEB.NVD.NIST.GOV/VIEW/NCP/REPOSITORY/; or
    c. Any generally recognized comparable standard that Contractor then applies to its own network and approved by DTS in writing.

Cisco Response: Cisco's Risk Assessment Policy permits Corporate Information Security to perform periodic vulnerability analysis, penetration testing, and risk assessments to determine areas of vulnerability and to initiate appropriate remediation. All tests are authorized and performed by InfoSec. Third parties or customers are not permitted to perform tests without prior InfoSec approval. Cisco's information security policies are designed to meet the ISO/IEC 27001 Information Security Management Systems (ISMS) requirements and are available on the Cisco intranet to all employees, contractors, consultants, temporary, and other workers at Cisco. In certain cases, Cisco has implemented more stringent internal controls to comply with legal, regulatory, or customer security requirements.

2. **Data security:** Contractor agrees to protect and maintain the security of the State of Utah data with protection that is at least as good as or better than that maintained by the State of Utah. These

security measures included but are not limited to maintaining secure environments that are patched and up to date with all appropriate security updates as designated, (ex. Microsoft Notification).

Cisco Response: Note that Cisco will comply with the Customer's policies while on the Customer's network or premises to the extent it does not violate Cisco's own policies. Otherwise, Cisco will comply with its own policies which generally align with those of the customers.

3. **Data Transmission**: Contractor agrees that any and all transmission or exchange of system application data with the State of Utah and/or any other parties expressly designated by the State of Utah, shall take place via secure means, (ex. HTTPS or FTPS).

Cisco Response: Cisco would like to discuss the applicability of exchanging system application data to this contract.

4. **Data Storage**: Contractor agrees that any and all State of Utah data will be stored, processed, and maintained solely on designated target servers approved of by DTS and that no State of Utah data at any time will be processed on or transferred to any portable or laptop computing device or any portable storage medium, unless such medium is part of the Contractor's designated backup and recovery process.

Cisco Response: Cisco would like to discuss the type of data that may be stored, processed, or maintained under this Contract. Changes may be requested, depending on our discussions, as Cisco may not be able to remain agile and have DTS approve each target server.

5. **Data Encryption**: Contractor agrees to store all State of Utah backup data as part of its designated backup and recovery process in encrypted form, using no less than 128 bit key.

Cisco Response: Cisco would like to discuss the type of data that may require a backup under this Contract. Changes may be requested, depending on our discussions.

6. **Password Protection**. Contractor agrees that any portable or laptop computer that has access to a State of Utah network, or stores any non-public State of Utah data is equipped with strong and secure password protection.

Cisco Response: Cisco would like to discuss the type of data that may require password protection under this Contract. Changes may be requested, depending on our discussions.

7. **Data Re-Use:** Contractor agrees that any and all data exchanged shall be used expressly and solely for the purpose enumerated in this Contract. Contractor further agrees that no State of Utah data of any kind shall be transmitted, exchanged or otherwise passed to other Contractors or interested parties except on a case-by-case basis as specifically agreed to in writing by DTS.

Cisco Response: Cisco agrees to the first sentence only; we need to be permitted to transfer or exchange with subcontractors who have agreed to substantially similar data re-use obligations of this contract. Our standard business and operating processes would be impeded significantly if we are required to obtain approval in writing each time we have a subcontractor who may need access to data.

8. **Data Destruction**: The Contractor agrees that upon termination of this Agreement it shall erase, destroy, and render unreadable all State of Utah data from all non-state computer systems and backups, and certify in writing that these actions have been completed within 30 days of the termination of this Agreement or within 7 days of the request of DTS, whichever shall come first.

Cisco Response: Cisco agrees with the modification of "*7 days*" to "*15 working days.*" In addition, please clarify in the first sentence that "*data will be destroyed upon written request from the Customer*." Also, to the extent this differs from Cisco's data destruction policy, Cisco's policy will prevail (note that our policy is generally in line or more stringent than those of our customers).

18. **NOTIFICATION AND DATA BREACHES:** Contractor agrees to comply with all applicable laws that require the notification of individuals in the event of unauthorized release of personally-identifiable information or other events requiring notification in accordance with *DTS Policy 5000-1250-PR1 Computer* Incident *Reporting Procedure* (copy available upon request). In the event of a data breach of any Contractor's security obligations or other event requiring notification under applicable law (Utah Code Annotated § 13-44-101 thru 301 et al), Contractor agrees at its own expense to assume responsibility for informing all such individuals in accordance with applicable laws and to indemnify, hold harmless and defend the State of Utah against any claims, damages, or other harm related to such

Notification Event.

Cisco Response: Cisco agrees, pending review of *DTS Policy 5000-1250-PR1 Computer Incident Reporting Procedure*. In addition, liability for breach of the contract and indemnification are covered in the WSCA-NASPO Master Agreement Terms and Conditions and elsewhere in this contract. As such, please delete the end of the last sentence starting with "*and to indemnify*."

19. CHANGE MANAGEMENT: Contractor agrees to comply with DTS Change Management Policy 4000-0004. This DTS policy requires that any work performed by the Contractor that has the potential to cause any form of outage, or modify the State's infrastructure architecture must first be reviewed by the DTS Change Management Committee, and coordinated accordingly. The DTS Project Manager will inform the Contractor if this change control requirement is applicable. Following this notification, any failure by the Contractor that causes outages or data security breaches caused by the Contractor as a direct result of failure to comply, will result in the Contractor's liability for the damages.

For reference purposes, the latest version of DTS Change Management Policy 4000-0004 is detailed at http://dts.utah.gov/policies/documents/4000-0004changemanagementpolicy.pdf.

Cisco Response: Cisco requests a copy of DTS Change Management Policy for review before providing final comments to this Section. Please note that Contractor's liability will be capped at the limitation of liability, and Cisco is not liable for lost data.

20. PUBLIC INFORMATION: Contractor agrees that the contract, related Sales Orders, and Invoices will be public documents, and may be available for distribution. Contractor gives the State express permission to make copies of the contract, related Sales Orders, and Invoices in accordance with the State of Utah Government Records Access and Management Act (GRAMA). Except for sections identified in writing and expressly approved by the State Division of Purchasing, Contractor also agrees that the Contractor's response to the solicitation will be a public document, and copies may be given to the public under GRAMA laws. The permission to make copies as noted will take precedence over any statements of confidentiality, proprietary information, copyright information, or similar notation.

Cisco Response: Agreed

21. CREDITING STATE IN ADVERTISING / PUBLICITY: Any publicity given to the project or services provided herein shall identify the State of Utah's managing agency as the sponsoring agency and shall not be released without prior written approval by that State agency's Project Manager.

Cisco Response: Agreed, with clarification that *"any such release shall be on prior written mutual agreement of the parties."*

22. STATE AGENCY WEB SITE BRANDING: The Contractor agrees to use the DTS logo, or a newer version if replaced in the future, on websites produced under terms of this contract. Contractor further agrees to allow a State agency to also utilize their own web site branding and logo, if requested by that State agency.

Cisco Response: Agreed, with clarification in the last sentence that *"any utilization of Cisco's branding will be per our logo/branding use requirements."*

23. ORDERING AND INVOICING: All orders will be shipped promptly in accordance with the delivery schedule. The Contractor will promptly submit invoices (within 30 days of shipment or delivery of services) to the State. The State contract number and/or the agency purchase order number shall be listed on all invoices, freight tickets, and correspondence relating to the contract order. The prices paid by the State will be those prices listed in the contract. The State has the right to adjust or return any invoice reflecting incorrect pricing.

Cisco Response: Cisco respectfully requests replacement of this Section with the terms in the current Cisco WSCA Data Communications AR-233. This Section would now be entitled Ordering, Delivery, and Invoicing:

23.1 After receipt and acceptance by Contractor of State's Purchase Order(s), Contractor will use commercially reasonable efforts to ship all direct purchase orders designated for shipment to U.S. locations within thirty (30) days for all products. Please note that the following circumstances may affect lead times: (i) new products purchased within the first three (3) months of release of the product which are subject to Contractor's then current published lead-times, (ii) third-party stand-

alone products which are not a component of equipment resold by Contractor, (iii) end-of-life products where the termination of the product has been announced by Contractor, (iv) products which have been line-stopped due to software discrepancies, reconfiguration, industry-wide product shortages, or alleged infringement claims, or (vi) situations where government rated orders create delays in lead-times.

Notwithstanding the foregoing, at any time when State states "expedite" on a Purchase Order or otherwise communicates to Contractor that a purchase order is to be expedited, Contractor shall use all commercially reasonable efforts to ensure the earliest possible delivery of such products.

23.2 Contractor will communicate scheduled shipping dates in the order acknowledgement and/or on cisco.com within three (3) business days after receipt of an electronic Purchase Order on cisco.com, provided, however, that in the event such notification is not received in this time period, State shall notify Contractor of the non-receipt, and Contractor's sole obligation with respect to such non-receipt shall be to promptly provide the information to the State after such notification.

23.3 If Contractor has reason to believe that the actual shipment date will occur later than the original shipment date acknowledged by Contractor for reasons caused by Contractor, Contractor shall use commercially reasonable efforts to promptly provide additional information to State including by electronic posting of the expected period of delay and, upon request, of the steps available, if any, to minimize the delay. If the extended delivery date is anticipated to be more than thirty (30) calendar days beyond the originally scheduled delivery date, the parties will work in good faith to resolve any ordering issues pursuant to the order escalation process.

23.4 Shipping terms are FOB destination, shipping and handling prepaid by Contractor. The method of shipment shall be consistent with the nature of the products and hazards of transportation. Acceptance by Purchaser shall be deemed to have occurred upon delivery of the applicable products to the applicable Purchaser. Title and risk of loss shall pass to Purchaser upon delivery.

23.5 If Purchaser requests delivery of products to Purchaser's forwarding agent or other representative, Purchaser assumes responsibility for compliance with applicable export laws and regulations.

23.6 Contractor is not liable for damage or penalty for delay in delivery or for failure to give notice of delay. Contractor shall not have any liability in connection with product shipment other than as set forth in this Section.

All sales are final. Except as provided in Contractor's Limited Warranty, Contractor only permits the return of un-opened products due to Contractor's shipping or order processing error, or damage in transit. No other returns are authorized under this contract. Warranty returns will not be subject to any restocking charges."

24. PROMPT PAYMENT DISCOUNT: Offeror may quote a prompt payment discount based upon early payment; however, discounts offered for less than 30 days will not be considered in making the award. Contractor shall list Payment Discount Terms on invoices. The prompt payment discount will apply to payments made with purchasing cards and checks. The date from which discount time is calculated will be the date a correct invoice is received or receipt of shipment, whichever is later; except that if testing is performed, the date will be the date of acceptance of the merchandise.

Cisco Response: Agreed

25. PAYMENT:

1. Payments are normally made within 30 days following the date the order is delivered or the date a correct invoice is received, whichever is later. After 60 days from the date a correct invoice is received by the appropriate State official, the Contractor may assess interest on overdue, undisputed account charges up to a maximum of the interest rate paid by the IRS on taxpayer refund claims, plus two percent, computed similarly as the requirements of Utah Code Annotated Section 15-6-3. The IRS interest rate is adjusted quarterly, and is applied on a per annum basis, on the invoice amount that is overdue.

Cisco Response: Cisco respectfully requests replacement of this Section with the terms in the current Cisco WSCA Data Communications AR-233.

"Upon and subject to credit approval by Contractor, payment is net thirty (30) days from invoice date and shall be made in U.S. currency. Invoices for products ordered without implementation services shall be

rendered by Contractor on or after the date of delivery of such products to the Purchaser. If, at any time, Purchaser is delinquent in payment, or is otherwise in breach of this contract, Contractor may, without prejudice to other rights, withhold shipment (including partial shipments) of any order or require Purchaser to prepay for further shipments. Any sum not paid by Purchaser when due shall bear interest until paid at a rate of 1 percent per month (12 percent per annum) or the maximum legal rate, whichever is less. Purchaser grants Contractor a security interest in products purchased under this contract to secure payment for those products purchased which security interest shall expire upon full payment in accordance with the terms. If requested by Contractor, Purchaser agrees to execute financing statements to perfect this security interest. Payments may be made via a State or political subdivision "Purchasing Card" to Fulfillment Partners under this contract."

2. The contract total may be changed only by written amendment executed by authorized personnel of the parties. Unless otherwise stated in the Contract, all payments to the Contractor will be remitted by mail, electronic funds transfer, or the State of Utah's purchasing card (major credit card). The State of Utah will not allow the Contractor to charge end users electronic payment fees of any kind.

Cisco Response: Agreed

3. The acceptance by the Contractor of final payment without a written protest filed with the State within ten (10) working days of receipt of final payment shall release the State from all claims and all liability to the Contractor for fees and costs of the performance of the services pursuant to this Contract.

Cisco Response: Agreed, with modification of "*ten (10) working days*" to "*twenty (20) working days.*"

4. Overpayment: The Contractor agrees that if during or subsequent to the contract performance, a CPA audit, or a State agency audit determines that payments were incorrectly reported or paid the State may adjust the payments. The Contractor shall, upon written request, immediately refund to DTS any such overpayments. The Contractor further agrees that the State shall have the right to withhold any or all-subsequent payments under this or other contracts that the Contractor may have with the State until recoupment of overpayment is made.

Cisco Response: Agreed, with 1) clarification that any subsequent audit must be within one (1) year after such contract performance, 2) Cisco confirms the audit results, and 3) deletion of the last sentence as Cisco's accounting systems cannot accommodate set offs.

5. Payment withholding: the Contractor agrees that the adequate reporting, record keeping, and compliance requirements specified in this contract are a material element of performance and that if the Contractor's record keeping practices, compliance, and/or reporting to DTS are not conducted in a timely and satisfactory manner, DTS may withhold part or all payments under this or any other contract until such deficiencies have been remedied. This includes, but is not limited to, Contractors failure to provide timely invoicing, and/or other requirements described elsewhere within this contract. In the event of the payment(s) being withheld, DTS agrees to provide ten (10) day advance Notice to the Contractor of the deficiencies that must be corrected in order to bring about the release of withheld payment. Contractor shall have ten (10) days thereafter to correct the cited reporting or record keeping practice deficiencies or the contract may be terminated.

Cisco Response: Cisco respectfully requests modifying this Section to the following:

*"**Payment withholding:** the Contractor agrees that the adequate reporting, record keeping, and compliance requirements specified in this contract are a material element of performance and that if the Contractor's record keeping practices, compliance, and/or reporting to DTS are not conducted in a timely and satisfactory manner and, after notice to Contractor by the State, Contractor will use commercially reasonable efforts to rectify the situation within fifteen (15) working days. This includes, but is not limited to, Contractors failure to provide timely invoicing, and/or other requirements described elsewhere within this contract."*

26. COPYRIGHT: The contractor agrees that any and all Deliverables prepared for the State of Utah as required by this contract, to the extent to which it is eligible under copyright law in any country, shall be deemed a work made for hire, such that all rights, title and interest in the work and Deliverables shall be exclusively owned by the State of Utah. State of Utah reserves a royalty-free, nonexclusive, and irrevocable license to reproduce, publish, or otherwise use and to authorize others to use for Federal or State Government purposes, such software, modifications and documentation. To the extent any Deliverable is deemed not to be, for any reason whatsoever, work made for hire, Contractor agrees to

assign and hereby assigns all right title and interest, including but not limited to copyright patent, trademark and trade secret, to such Deliverables, and all extensions and renewals thereof, to the State of Utah. Contractor further agrees to provide all assistance reasonably requested by the State of Utah in the establishment, preservation, and enforcement of its rights in such Deliverables, without any additional compensation to Contractor. Contractor agrees to and hereby, to the extent permissible, waives all legal and equitable rights relating to the Deliverables, including without limitation any and all rights of identification of authorship and any and all rights of approval, restriction or limitation on use or subsequent modifications.

Cisco Response: Cisco Professional/Advance Services will be provided per the Master Services Agreement ("MSA Terms"), included in the Additional Terms and Conditions. The MSA Terms, which covers ownership in Section 12, will be added as an Attachment to the WSCA-NASPO Master Agreement Terms and Conditions and shall replace this Section. Therefore, Cisco respectfully requests deletion of this Section.

27. OWNERSHIP, PROTECTION AND USE OF RECORDS: Except for confidential medical records held by direct care providers, the State shall own exclusive title to all information gathered, reports developed, and conclusions reached in performance of this Contract. The Contractor may not use, except in meeting its obligations under this contract, information gathered, reports developed, or conclusions reached in performance of this Contract without the express written consent of the State. The improper use or disclosure of any information concerning a State of Utah client, or a State of Utah employee for any purpose not directly connected with the administration of the State, or the Contractor's responsibilities with respect to services purchased under this agreement, is prohibited except on written consent of the state agency employee, state agency client, their attorney, or their responsible parent or guardian. The Contractor will be required to sign a Confidential Information Certification form in situations where they will be given access to confidential computerized records. The Contractor agrees to maintain the confidentiality of records it holds as agent for the State as required by Government Records Access and Management Act ("GRAMA"), or other applicable federal or state law. The State of Utah shall own and retain unlimited rights to use, disclose, or duplicate all information and data (copyrighted or otherwise) developed, derived, documented, stored, or furnished by the Contractor under the Contract. The Contractor, and any subcontractors under its control, expressly agrees not to use confidential client, or confidential federal, state, or local government data, without prior written permission from the State of Utah Project Manager and appropriate officials of the State Agency.

Cisco Response: Cisco Professional/Advance Services will be provided per the Master Services Agreement ("MSA Terms"), included in the Additional Terms and Conditions. The MSA Terms, which covers ownership in Section 12, will be added as an Attachment to the WSCA-NASPO Master Agreement Terms and Conditions and shall replace this Section. Also, Confidentiality terms are included in the WSCA-NASPO Master Agreement Terms and Conditions. Therefore, Cisco respectfully requests deletion of this Section.

28. OWNERSHIP, PROTECTION, AND USE OF CONFIDENTIAL FEDERAL, STATE, OR LOCAL GOVERNMENT INTERNAL BUSINESS PROCESSES AND PROCEDURES: The improper use or disclosure by any party of protected internal Federal or State business processes, polices, procedures, or practices is prohibited. Confidential federal or state business processes, policies, procedures, or practices shall not be divulged by the Contractor, Contractor's employees, or their Subcontractors, unless prior written consent has been obtained in advance from the State of Utah Project Manager.

Cisco Response: Agreed, with the modification of changing the second sentence to a mutual obligation.

29. OWNERSHIP, PROTECTION, AND RETURN OF DOCUMENTS AND DATA UPON CONTRACT TERMINATION OR COMPLETION: All documents and data pertaining to work required by this contract will be the property of the State and must be delivered to the State within 30 working days after termination or completion of the contract, regardless of the reason for contract termination, and without restriction or limitation to their future use. Any State data that may be returned under provisions of this clause must either be in the format as originally provided, or in a format that is readily usable by the State or that can be formatted in a way that it can be used. Costs for all of these described items will be considered as included in the basic contract compensation of the work described used by the State.

Cisco Response: Cisco Professional/Advance Services will be provided per the Master Services Agreement ("MSA Terms"), included in the Additional Terms and Conditions. The MSA Terms, which covers ownership

in Section 12, will be added as an Attachment to the WSCA-NASPO Master Agreement Terms and Conditions and shall replace this Section. Therefore, Cisco respectfully requests deletion of this Section.

30. CONFIDENTIALITY: Contractor, and anyone for whom the Contractor may be liable, must maintain the confidentiality of any non-public personal information. Personal information includes, but is not limited to, names, social security numbers, birth dates, address, credit card numbers and financial account numbers. The State reserves the right to identify additional reasonable types or categories of information that must be kept confidential by the Contractor and anyone for whom the Contractor may be liable. This duty of confidentiality shall be ongoing and survive the term of this contract.

Cisco Response: Cisco respectfully requests deletion of this Section as, given the scope of this contract, we should not have access to any personal information. Confidentiality will then be covered in the WSCA-NASPO Master Agreement Terms and Conditions.

31. TERMINATION UPON DEFAULT: In the event this contract is terminated as a result of a default by the Contractor, the State may procure or otherwise obtain, upon such terms and conditions as the State deems appropriate, services similar to those terminated, and Contractor shall be liable to the State for any and all damages arising there from, including, but not limited to, attorneys' fees and excess costs incurred by the State in obtaining similar services.

Cisco Response: Cisco respectfully requests deletion of this Section. Cisco cannot agree to be liable for the additional items listed in this Section. Any remedies are otherwise set forth in the WSCA-NASPO Master Agreement Terms and Conditions.

32. PROCUREMENT ETHICS: The Contractor understands that a person who is interested in any way in the sale of any supplies, services, construction, or insurance to the State of Utah is violating the law if the person gives or offers to give any compensation, gratuity, contribution, loan or reward, or any promise thereof to any person acting as a procurement officer on behalf of the State, or who in any official capacity participates in the procurement of such supplies, services, construction, or insurance, whether it is given for their own use or for the use or benefit of any other person or organization (63G-6-1002, Utah Code Annotated, 1953, as amended).

Cisco Response: Agreed

33. WORKERS' COMPENSATION: The Contractor shall furnish proof to the State, upon request and maintain during the life of this contract, workers' compensation insurance for all its employees as well as any subcontractor employees related to this contract.

Cisco Response: Cisco respectfully requests that this Section be modified to the following to eliminate ambiguity:

The Contractor shall furnish proof to the State, upon request, and maintain during the life of this contract, workers' compensation insurance for all its employees who perform work governed by this Agreement. The Contractor shall also undertake reasonable efforts to furnish proof to the State, upon request, of workers' compensation insurance coverage for any subcontractor employees who perform work governed by this Agreement.

34. LIABILITY INSURANCE: The Contractor agrees to provide and to maintain during the performance of the contract, at its sole expense, a policy of liability insurance. The limits of the policy shall be no less than $1,000,000.00 for each occurrence and $3,000,000.00 aggregate.

It shall be the responsibility of the Contractor to require any of their Subcontractor(s) to secure the same insurance coverage as prescribed herein for the Contractor.

Cisco Response: Insurance terms shall be per the terms of the WSCA-NASPO Master Agreement Terms and Conditions. Therefore, Cisco respectfully requests deletion of this section (and Section 43).

35. ENTIRE AGREEMENT: This Agreement, including all Attachments, and documents incorporated hereunder, and the related State Solicitation constitutes the entire agreement between the parties with respect to the subject matter, and supersedes any and all other prior and contemporaneous agreements and understandings between the parties, whether oral or written. The terms of this Agreement shall supersede any additional or conflicting terms or provisions that may be set forth or printed on the Contractor's work plans, cost estimate forms, receiving tickets, invoices, or any other related standard

forms or documents of the Contractor that may subsequently be used to implement, record, or invoice services hereunder from time to time, even if such standard forms or documents have been signed or initialed by a representative of the State. The parties agree that the terms of this Agreement shall prevail in any dispute between the terms of this Agreement and the terms printed on any such standard forms or documents, and such standard forms or documents shall not be considered written amendments of this Agreement.

Cisco Response: Agreed

36. **SURVIVORSHIP**: This paragraph defines the specific contractual provisions that will remain in effect after the completion of or termination of this contract, for whatever reason: (a) State of Utah Standard IT Terms and Conditions # 2, Contract Jurisdiction, Choice of Law, and Venue; (b) State of Utah Standard IT Terms and Conditions # 17, Secure Protection and Handling of Data; (c) State of Utah Standard IT Terms and Conditions # 18, Notification and Data Breaches; (d) State of Utah Standard IT Terms and Conditions # 26, Copyright; (e) State of Utah Standard IT Terms and Conditions #27, Ownership, Protection, and Use of Records, including Residuals of such records; and (f) State of Utah Standard IT Terms and Conditions # 28, Ownership, Protection, and Use of Confidential Federal, State, or Local Government Internal Business Processes, including Residuals of such confidential business processes; (g) State of Utah Standard IT Terms and Conditions # 29, Ownership, Protection, and Return of Documents and Data Upon Contract Termination or Completion; and (h) State of Utah Standard IT Terms and Conditions # 30, Confidentiality.

Cisco Response: Agreed; however, after negotiation of the final terms, this Section should be reviewed to ensure appropriate Section references are included.

37. **WAIVER**: The waiver by either party of any provision, term, covenant or condition of this Contract shall not be deemed to be a waiver of any other provision, term, covenant or condition of this Contract nor any subsequent breach of the same or any other provision, term, covenant or condition of this Contract.

Cisco Response: Agreed

If professional services are applicable to this solicitation/contract, the following terms and conditions apply:

Cisco Response: Cisco Professional/Advance Services will be provided per the Master Services Agreement ("MSA Terms"), included in the Additional Terms and Conditions. The MSA Terms will be added as an Attachment to the WSCA-NASPO Master Agreement Terms and Conditions and shall replace the below Sections, except for Section 43. With regard to Section 43, Insurance terms, this is redundant to terms in the WSCA-NASPO Master Agreement Terms and Conditions. Therefore, Cisco respectfully requests deletion of the Sections below.

38. **TIME:** The Contractor shall complete the scope of services work in a manner to achieve any milestones identified in the procurement documents related to this Contract and the attachments to this Contract. The full scope of services work shall be completed by any applicable deadline stated in the solicitation.

Cisco Response: See comment above Section 38.

39. **TIME IS OF THE ESSENCE:** For all work and services under this Contract, time is of the essence and Contractor shall be liable for all damages to the State of Utah and anyone for whom the State of Utah may be liable, as a result of the failure to timely complete the scope of work required under this Contract.

Cisco Response: See comment above Section 38.

40. **CHANGES IN SCOPE:** Any changes in the scope of the services to be performed under this Contract shall be in the form of a written amendment to this Contract, mutually agreed to and signed by duly authorized representatives of both parties, specifying any such changes, fee adjustments, any adjustment in time of performance, or any other significant factors arising from the changes in the scope of services.

Cisco Response: See comment above Section 38.

41. **PERFORMANCE EVALUATION:** The State of Utah may conduct a performance evaluation of the Contractor's services, including specific personnel of the Contractor. References in the Contract to Contractor shall include Contractor, Contractor's subcontractors, or subconsultants at any tier, if any.

Results of any evaluation will be made available to the Contractor.

Cisco Response: See comment above Section 38.

42. WAIVERS: No waiver by the State or Contractor of any default shall constitute a waiver of the same default at a later time or of a different default.

Cisco Response: See comment above Section 38.

43. INSURANCE:

1. To protect against liability, loss and/or expense in connection with the performance of services described under this Contract, the Contractor shall obtain and maintain in force during the entire period of this Contract without interruption, at its own expense, insurance as listed below from insurance companies authorized to do business in the State of Utah and with an A.M. Best rating as approved by the State of Utah Division of Risk Management.
2. The following are minimum coverages that may be supplemented by additional requirements contained in the solicitation for this Contract or provided in an Attachment to this Contract; if no insurance limits are identified in the solicitation, insurance minimums will default to Section 44. Liability Insurance Requirements:
   (1) Worker's Compensation Insurance and Employers' Liability Insurance. Worker's compensation insurance shall cover full liability under the worker's compensation laws of the jurisdiction in which the service is performed at the statutory limits required by said jurisdiction.
   (2) Professional liability insurance in the amount as described in the solicitation for this Contract, if applicable.
   (3) Any other insurance described in the solicitation for this Contract, if applicable.
3. Any type of insurance or any increase of limits of liability not described in this Contract which the Contractor requires for its own protection or on account of any statute, rule, or regulation shall be its own responsibility, and shall be provided at Contractor's own expense.
4. The carrying of insurance required by this Contract shall not be interpreted as relieving the Contractor of any other responsibility or liability under this Contract or any applicable law, statute, rule, regulation, or order.

Cisco Response: Insurance terms shall be per the terms of the WSCA-NASPO Master Agreement Terms and Conditions. As such, Cisco respectfully requests deletion of this Section.

44. STANDARD OF CARE: The services of Contractor and its subcontractors and subconsultants at any tier, if any, shall be performed in accordance with the standard of care exercised by licensed members of their respective professions having substantial experience providing similar services which similarities include the type, magnitude and complexity of the services that are the subject of this Contract. The Contractor shall be liable to the State of Utah for claims, liabilities, additional burdens, penalties, damages or third party claims (i.e. another Contractor's claim against the State of Utah), to the extent caused by wrongful acts, errors or omissions that do not meet this standard of care.

Cisco Response: See comment above Section 38.

45. STATE REVIEWS, LIMITATIONS: The right of the State to perform plan checks, plan reviews, other reviews and/or comment upon the services of the Contractor, as well as any approval by the State, shall not be construed as relieving the Contractor from its professional and legal responsibility for services required under this Contract. No review by the State or any entity/user, approval or acceptance, or payment for any of the services required under this Contract shall be construed to operate as a waiver by the State of any right under this Contract or of any cause of action arising out of the performance or nonperformance of this Contract, and the Contractor shall be and remain liable to the State in accordance with applicable law for all damages to the State caused by the wrongful acts, errors and/or omissions of the Contractor or its subcontractors or subconsultants at any tier, if any.

Cisco Response: See comment above Section 38.

Appendix C — Additional Vendor Terms and Conditions

End User License Agreement (EULA)

Cisco Systems, Inc. or its affiliate licensing the software ("Cisco") is willing to license this software to you only upon the condition that you purchased the software from an approved source and that you accept all of the terms contained in this end-user license agreement plus any additional limitations on the license set forth in a supplemental license agreement accompanying the product, available at the time of your order, or posted on the Cisco website at WWW.CISCO.COM/GO/TERMS (collectively, the "agreement"). To the extent of any conflict between the terms of this end-user license agreement and any supplemental license agreement, the supplemental license agreement shall apply. By downloading, installing, or using the software, you are representing that you purchased the software from an approved source and binding yourself to the agreement. if you do not agree to all of the terms of the agreement, then Cisco is unwilling to license the software to you and (a) you may not download, install, or use the software, and (b) you may return the software (including any unopened cd package and any written materials) for a full refund, or (c), if the software and written materials are supplied as part of another product, you may return the entire product for a full refund. Your right to return and refund expires 30 days after purchase from an approved source, and applies only if you are the original and registered end user purchaser. For the purposes of this end-user license agreement, an "approved source" means (a) Cisco; or (b) a distributor or systems integrator authorized by Cisco to distribute/sell Cisco equipment, software,and services within your territory to end users; or (c) a reseller authorized by any such distributor or systems integrator in accordance with the terms of the distributor's agreement with Cisco to distribute/sell the Cisco equipment software and services within your territory to end users.

Please note that the remaining license terms are addressed in the WSCA – NASPO Master Agreement Terms and Conditions.

Please note that the Master Services Agreement below is the same agreement utilized in our current Cisco WSCA Data Communications AR-233 contract, with updates to certain terminology.

Master Services Agreement

This Master Services Agreement governs all Orders for Services placed under the WSCA NASPO Master Agreement Terms and Conditions ("WSCA Master Agreement").

This Agreement is entered into between Cisco Systems, Inc. ("Cisco"), a California corporation having its principal place of business at 170 West Tasman Drive, San Jose, California, 95134 and the WSCA-NASPO Cooperative Purchasing Organization LLC ("WSCA"), on behalf of their Public Sector Customers formed under the laws of United States ("Customer") having its principal place of business at State of Utah, Division of Purchasing and General Services, State Office Building, Capitol Hill, Room 3150, Salt Lake City, UT 84114-1061, United States, and is entered into as of the date of last signature below (the "Effective Date").

This Master Services Agreement consists of (i) this signature page, (ii) the Master Services Agreement Terms and Conditions (including the Exhibits), and (iii) the Services Descriptions of the Services at cisco.com that the WSCA Customer may elect to purchase, which are incorporated in this Agreement by this reference.

The parties have caused this Agreement to be duly executed. Each party warrants and represents that its respective signatories whose signatures appear below are on the date of signature authorized to execute this Agreement.

_____ _____

{Insert Signature Boxes}

Master Services Agreement - Terms and Conditions

1. **Definitions** are those set out in the Exhibit A, Glossary of Terms at the end of the Agreement.
2. **Scope**. This Agreement describes the terms and conditions for (a) Purchases by Customer of Services, and (b) delivery by Cisco of the Services according to the options ordered by Customer or otherwise provided by Cisco to Customer. Cisco will provide Services for Products and Customer will be entitled to receive Services for which (i) the applicable Services fees have been paid, (ii) a valid Software license has been granted, and (iii) Customer provides information requested by Cisco such as valid serial numbers, site location, contract number, and Product type.
3. **Orders**. Where payment is directly to Cisco or its Fulfilment Partners, Customer shall, upon and subject to credit approval by Cisco, purchase Services by issuing a Purchase Order. Each Purchase Order must be signed, if requested by Cisco, or (in the case of electronic transmission) sent, by an authorized representative, indicating the specific Services, quantity, price, total purchase price, shipping instructions, requested delivery dates, bill-to and ship-to addresses, tax exempt certifications, if applicable, contract reference if any, and any other special instructions. No contingency contained on any Purchase Order shall be binding upon Cisco. The terms of this Agreement shall apply, regardless of any additional or conflicting terms on any Purchase Order or other correspondence or documentation submitted by Customer to Cisco, and any such additional or conflicting terms are deemed rejected by Cisco.
4. **Pricing**. For Direct Purchases, and subsequent Equipment List renewals, prices for Services shall be (a) those specified in Cisco's then-current Price List less any applicable contract discount in effect under the WSCA Master Agreement at the time of acceptance of the Purchase Order by Cisco, or (b) those set forth in a written price quotation submitted by Cisco or its Fulfilment Partner, if at or below the stated contract discount. All stated prices are exclusive of taxes, fees, and duties or other amounts in accordance with the WSCA Master Agreement. Any taxes related to Services purchased pursuant to this Agreement shall be paid by Customer or Customer shall present an exemption certificate acceptable to the taxing authorities. Applicable taxes shall be billed as a separate item on the invoice, to the extent possible. In the event that Customer is unable to provide valid and applicable serial number(s) for Product and Cisco agrees to provide Services, then Service fees payable by Customer shall be at Cisco's then-current time and materials or non-contract service rates.

   Subject to the price discount floor established by Cisco under the WSCA Master Agreement, for Indirect Purchases, Fulfillment Partners are free to determine their resale prices unilaterally. Customer understands that no employee or representative of Cisco or anyone else has any authority to determine such resale prices, or to limit the Fulfillment Partners' pricing discretion with respect to Services.
5. **Payment**. For Purchases of Services, upon and subject to credit approval by Cisco, payment terms shall be net thirty (30) days from the date of invoice. Unless otherwise agreed by Cisco, all payments shall be made in U.S. currency. Any sum not paid by Customer when due shall bear interest from the due date in accordance with the terms for interest on late payments under the WSCA Master Agreement.
6. **Invoicing**. Fees for Services, other than those for which a SOW is required, shall be invoiced in advance of delivery of Services. The timing of invoices for Services provided pursuant to a SOW shall be set forth in the respective SOW.
7. **Term and Termination.**

   (a) The term of any service order shall commence on the Effective Date of the Order and shall continue for a period of one (1) year, or such other multi-year period as set forth in the purchase order or SOW. Such term will be renewed automatically for successive one (1) year terms unless either party notifies the other of its intent to terminate at least sixty (60) days prior to the expiration of the then current term.

   (b) The term of an Equipment List shall commence on the date set forth on such.

   (c) Equipment List, which may be up to sixty (60) days following the date of Purchase Order acceptance by Cisco. The term of an Equipment List shall be for a period of one (1) year and shall be renewed automatically for successive one (1) year terms, unless either party notifies the other of its intent to terminate at least sixty (60) days prior to the expiration of the then current one (1) year term.

(d) The term of each SOW shall be stated in the SOW.

This Master Service Agreement may be terminated in accordance on the same terms as set forth in the WSCA Master Agreement. Any Equipment List or SOW may be terminated immediately by either party upon written notice:

(i) if the other party breaches any of the material provisions of this Agreement and the breach is not capable of being cured, or after providing thirty (30) days written notice to the breaching party if the breaching party fails to cure such breach within such period.

(ii) if: (a) the other party ceases to carry on business as a going concern; or (b) the other party becomes or may become the object of the institution of voluntary or involuntary proceedings in bankruptcy or liquidation; or (c) a receiver or similar officer is appointed with respect to the whole or a substantial part of the other party's assets; or (d) an event similar to any of the foregoing occurs under applicable law with respect to the other party.

(iii) if the other party assigns or transfers any of the rights or responsibilities granted under this Agreement or any Equipment List or SOW in breach of Section 16.

If Services fees are not paid when due and payment has not been received within thirty (30) days after notice from Cisco of such past due payment, Cisco may withhold the provision of Services until all amounts past due are paid in full, and/or terminate immediately this Agreement, any Equipment List, and SOW.

(e) Cisco reserves the right to make changes to the scope and content of the Services or part thereof, including terminating the availability of a given Service, at any time upon ninety (90) days' prior notice. Such changes will become effective upon renewal of the affected Equipment Lists and SOWs. If Customer does not agree to a change of scope or content, Customer may terminate any affected Equipment List or SOW by notifying Cisco at least sixty (60) days prior to the expiration of the then current one (1) year term of the Equipment List or SOW. In such case, Cisco shall continue to provide Services until the next expiration date of the affected Equipment List or SOW.

(f) Each Equipment List and SOW hereunder shall terminate immediately upon termination of the Agreement.

(g) Upon termination of the Agreement, any Equipment List, or SOWs, Customer shall pay Cisco for all work performed under the affected Equipment Lists or SOWs up to the effective date of termination at the agreed-upon prices, fees, and expense reimbursement rates.

(h) Firm orders for services under this Master Services Agreement placed and accepted prior to expiration of the contract term, (even if involving a multi-year commitment) remain valid in accordance with the contract terms which shall remain binding as to such prior orders only for the term stated therein, and shall not otherwise constitute an extension of the Master Services Agreement.

8. Confidentiality. Customer and Cisco agree that in connection with this Agreement and their relationship, they may obtain Confidential Information. The receiving party shall at all times keep in trust and confidence all such Confidential Information, and shall not use such Confidential Information other than as expressly authorized by the disclosing party under this Agreement, nor shall the receiving party disclose any such Confidential Information to third parties without the disclosing party's written consent. Notwithstanding the above, Cisco shall be authorized to disclose Customer's Confidential Information to contractors or employees of a Cisco entity who have a legitimate business need to have access to such information. Except to the extent retention is otherwise required by law for records retention purposes, the receiving party shall immediately return to the disclosing party all Confidential Information (including copies thereof) in the receiving party's possession, custody, or control upon termination or expiration at any time and for any reason of this Agreement. The obligations of confidentiality shall not apply to information which (a) has entered the public domain, except where such entry is the result of the receiving party's breach of this Agreement; (b) prior to disclosure hereunder was already rightfully in the receiving party's possession; (c) subsequent to disclosure hereunder is obtained by the receiving party on a non-confidential basis from a third party who has the right to disclose such information to the receiving party. The receiving party will be authorized to disclose Confidential Information pursuant to a valid order issued by a court or government agency, provided that the receiving party provides (i) prior written notice to the disclosing party of such obligation and (ii) the opportunity to oppose such disclosure.

Neither party shall disclose, advertise, or publish the detailed terms and conditions of an SOW or detailed ordering document or deliverables in conjunction therewith under this Agreement without the prior written consent of the other party. Any press release or publication regarding such documents or deliverables under this Agreement are presumed by the parties to contain confidential information and is subject to prior review and written approval of the parties. In such event, only the invoice will be presumed public information. Notwithstanding confidentiality of the detailed ordering documents and deliverables, the parties shall be deemed to have given their consent to release of this Agreement.

9. **Warranty**. All services provided hereunder shall be performed in a workmanlike manner in accordance with industry standards expected of a company providing professional services in the networking industry. Except as specified in this section, Cisco hereby disclaims and customer waives all representations, conditions, and warranties (whether express, implied, or statutory), including without limitation, any warranty or condition (a) of merchantability, fitness for a particular purpose, non-infringement, title, satisfactory quality, accuracy, (b) arising from any course of dealing, course of performance, or usage in the industry. To the extent an implied warranty cannot be disclaimed, such warranty is limited in duration to the applicable express warranty period. Customer's sole and exclusive remedy for breach of warranty shall be, at Cisco's option, re-performance of the services; or termination of this agreement or the applicable equipment list or SOW and return of the portion of the service fees paid to Cisco by customer for such non-conforming services.

10. **Limitation of Liability and Consequential Damages Waiver.**

    Except for the general indemnity provision set forth in the WSCA Master Agreement, all liability of Cisco, its affiliates, officers, directors, employees, agents, and suppliers collectively for claims arising under this agreement or otherwise howsoever arising shall be limited to the greater of (i) the money paid to Cisco for services under this agreement during the twelve (12) month period preceding the event or circumstances first giving rise to such liability or (ii) one hundred thousand ($100,000) U.S. dollars. This limitation of liability is cumulative and not per-incident (i.e., the existence of two or more claims will not enlarge this limit).

    In the case of transactional advanced services performed under a SOW, the liability of Cisco shall be limited to the amount paid by customer to Cisco pursuant to the relevant SOW during the twelve (12) months preceding the event or circumstances giving rise to such liability.

    Subject to customer's breach of Section 11 (license), in no event shall either party, its respective affiliates, officers, directors, employees, agents, or suppliers be liable for any special, incidental, indirect or consequential damages, or lost revenue, lost profits, or lost or damaged data, whether arising in contract, tort (including negligence), or otherwise, even if such party has been informed of the possibility thereof.

11. **License**. Cisco grants to Customer a nonexclusive and non-transferable license to use for Customer's internal business use (a) Software provided as a result of Services (b) the Deliverables specified in each SOW (in object code form if software), and (c) Data Collection Tools. This license grant does not include the right to sublicense and is non-transferable.

    This license shall be governed by (i) the terms and conditions attached to the Software or, in the absence of such terms, by the license posted at http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html and (ii) the Agreement.

    Customer agrees that it is licensed to use Software: (1) only on Hardware covered under this Agreement; or (2) in the case of Application Software, on third-party hardware, (except as otherwise authorized in the Software documentation); or (3) in the case of Data Collection Tools, in object code form only, on the Data Collection Tool on which such Software is provided.

    The license is perpetual, provided Customer is not otherwise in breach of this license. Notwithstanding the above, for Data Collection Tools the license is valid until the earlier of: (i) the expiration or termination of the Service under which the Data Collection Tool was provided; or (ii) Cisco's request to Customer that the Data Collection Tool(s) be returned to Cisco.

    Except as expressly authorized, Customer shall not (and shall not permit a third party to): download more than one copy of the Software, copy, in whole or in part, any Software, Deliverable or Data Collection Tool, make error corrections or otherwise modify, decompile, decrypt, reverse engineer,

disassemble, or otherwise reduce all or any portion of any Software, Deliverable, or Data Collection Tool which is software to human-readable form; or transfer, sublicense, rent, lease, distribute, sell, or create derivative works of any Deliverables.

When Customer updates or upgrades a copy of Software to a new release, Customer shall not use (except for a limited period of parallel testing) the new Software release and the corresponding copy of the previous Software release concurrently. Under no circumstances shall the previous release be re-used or transferred to any other device(s).

12. **Ownership.** Cisco shall at all times retain all right, title, and interest in and to all pre-existing Intellectual Property owned by Cisco as of the Effective Date and all Intellectual Property in and to the Services, Cisco Products, Deliverables, and Data Collection Tools or other Intellectual Property provided or developed by Cisco or a third party on Cisco's behalf thereafter. Customer shall at all times retain all right, title, and interest in and to all pre-existing Intellectual Property owned by Customer as of the Effective Date and all Intellectual Property that is developed by Customer or by a third party on Customer's behalf thereafter without the benefit of any of Cisco's Intellectual Property. Third Party Products shall at all times be owned by the applicable third party.

13. **Force Majeure**. Except for the obligation to pay monies due and owing, neither party shall be liable for any delay or failure in performance due to events outside the defaulting party's reasonable control, including without limitation acts of God, earthquake, labor disputes, industry wide shortages of supplies, actions of governmental entities, riots, war, terrorism, fire, epidemics, or delays of common carriers or other circumstances beyond its reasonable control. The obligations and rights of the defaulting party shall be extended for a period equal to the period during which such event prevented such party's performance.

14. **Applicable law and Jurisdiction**. Notwithstanding the foregoing, either party may seek interim or temporary injunctive relief in any court of appropriate jurisdiction with respect to any alleged breach of such party's intellectual property or proprietary rights.

    a. WSCA Master Services Agreement: This Agreement and disputes hereunder solely between State acting on behalf of WSCA and Cisco shall be construed in accordance with the laws of the State of Utah. Venue for any claim, dispute, or action concerning this Agreement shall be in Utah.

    b. Participating Addendum and Service Orders Placed Under the Participating Addendum: To the extent that both parties have mutually agreed to be bound by such laws under the terms of the *Participating Addendum*, each *Participating Addendum* and any dispute under this Agreement based upon a performance under a *Participating Addendum* shall be governed by the laws of the Participating State. Venue for any claim, dispute, or action concerning an order placed against a *Participating Addendum* or the effect of a *Participating Addendum* shall be in the Participating State.

    c. The parties specifically disclaim the application of the U.N. Convention on Contracts for the International Sale of Goods to the interpretation or enforcement of this Agreement.

15. **Export Control**. Customer shall comply with such laws and regulations governing use, export, re-export, and transfer of Cisco Products and technology and will obtain all required U.S. and local authorizations, permits, or licenses. Information regarding compliance with U.S. use, export, re-export, and transfer laws may be found at: http://www.cisco.com/wwl/export/compliance_provision.html.

16. **Assignment**. Neither party may assign or delegate its rights or obligations under this Agreement without the prior written consent of the other, such consent not to be unreasonably withheld or delayed, provided that any such assignment shall not relieve the assigning entity of any obligation to pay monies that were owed prior to the date of the assignment. Notwithstanding the foregoing, (a) either party may, without the other party's consent, assign or delegate its rights or obligations under this Agreement to its parent or majority-owned subsidiary company of sufficient net worth to meet any potential liability under this Agreement, and (b) Cisco may, without Customer's consent, assign the right to receive any amount due.

17. **Subcontracting.** Cisco reserves the right to subcontract Services to a third party organization including Fulfilment Partners or Servicing Subcontractors (as defined in the WSCA Master Agreement) to provide Services to Customer; provided that invoicing and/or payments will only be handled by and through Cisco and its authorized Fulfilment Partners. Any such subcontract shall not relieve Cisco of any of its obligations under this Agreement.

If Contractor or its Fulfillment Partners are using servicing subcontractors for the performance of local marketing, maintenance, and/or technical support services in accordance with the terms and conditions of this Contract, servicing subcontractors may not directly accept purchase orders or payments for products or services from Purchasers under the terms and conditions of the contract. Only Contractor or Fulfillment Partners authorized by Cisco may directly accept purchase orders, invoice, or receive payments for products or services under the terms and conditions of the contract. The authorized Purchaser has the option of choosing whether to purchase the associated OEM maintenance and/or training to support the equipment purchased.

18. **Inventory Review**. From time-to-time Cisco may perform an inventory review of Customer's installed base and review serial numbers and other records (upon reasonable advance notice) to validate entitlement. Cisco will charge a Service fee if it finds that unauthorized Services are being provided. This Service fee includes amounts which should have been paid, interest, and attorneys' and audit fees. Attorneys' and audit fees will only be payable by the customer where the discrepancy exceeds 5 percent of the amount otherwise due and payable. Cisco requires that Customer take all necessary action (for example, disabling passwords) to ensure that any former employees and contractors do not access or use the Service.

19. **Notices**. Notwithstanding anything contained in the Agreement to the contrary, all notices required or permitted under this Agreement will be in writing and will be deemed given: (a) when delivered personally; (b) when sent by confirmed facsimile or electronic mail (in the case of Cisco to Agreement-notice@cisco.com), (provided that the original document is placed in air mail/air courier or delivered personally, within seven (7) days of the facsimile electronic notice); (c) three (3) days after having been sent by registered or certified mail, return receipt requested, postage prepaid (or six [6] days for international mail); or (d) one (1) day after deposit with a commercial express courier specifying next day delivery (or two (2) days for international courier packages specifying 2-day delivery), with written verification of receipt. All communications will be sent to the addresses set forth on the cover sheet of this Agreement or such other address as may be designated by a party by giving written notice to the other party pursuant to this paragraph. Notwithstanding the above, notices regarding general changes in pricing, policies, or programs may also be by posting on Cisco.com or by email or fax.

20. **Entire Agreement**. This Master Services Agreement, in addition to the general provisions of the WSCA Master Agreement pertinent to Services, is the complete agreement between the parties concerning the subject matter of this Agreement and replaces any prior oral or written communications between the parties, except as agreed between the parties. There are no conditions, understandings, agreements, representations, or warranties expressed or implied, that are not specified herein. This Agreement may only be modified by a written document executed by the parties hereto.

21. **No Waiver**. The waiver by either party of any right provided under this Agreement shall not constitute a subsequent or continuing waiver of such right or of any other right under this Agreement.

22. **Severability**. In the event that one or more terms of this Agreement becomes or is declared to be illegal or otherwise unenforceable by any court of competent jurisdiction, each such term shall be null and void and shall be deemed deleted from this Agreement. All remaining terms of this Agreement shall remain in full force and effect. Notwithstanding the foregoing, if this paragraph is invoked and, as a result, the value of this Agreement is materially impaired for either party, as determined by such party in its sole discretion, then the affected party may terminate this Agreement by written notice with immediate effect to the other.

23. **Attorneys' Fees**. In any suit or proceeding relating to this Agreement, the prevailing party will have the right to recover from the other its costs and reasonable fees and expenses of attorneys, accountants, incurred in connection with the suit or proceeding, including costs, fees, and expenses upon appeal, separately from and in addition to any other amount included in such judgment. This provision is intended to be severable from the other provisions of this Agreement, and shall survive expiration or termination and shall not be merged into any such judgment unless the judgment expressly precludes survivability.

24. **No Agency**. This Agreement does not create any agency, partnership, joint venture, or franchise relationship. No employee of either party shall be or become, or shall be deemed to be or become, an employee of the other party by virtue of the existence or implementation of this Agreement. Each party

hereto is an independent contractor. Neither party shall assume or create any obligation of any nature whatsoever on behalf of the other party or bind the other party in any respect whatsoever.

25. **Counterparts**. This Agreement may be executed in two counterparts, each of which shall be deemed an original and together which shall constitute one and the same instrument. A validly executed counterpart that is delivered by one party to the other via electronic transmission (a "Counterpart Image") shall be valid and binding to the same extent as one delivered physically, provided that the valid signature is clearly visible in the Counterpart Image. In the event that a party delivers a Counterpart Image in place of an originally-executed counterpart, such party shall retain the originally-executed counterpart in its files for at least the duration of the Term hereof.
26. **Headings**. Headings of sections have been added solely for convenience of reference and shall not be deemed part of this Agreement.
27. **Survival**. Sections 5 (Payment), 7 (Term and Termination), 8 (Confidentiality), 0 (Warranty), 0 (Limitation of Liability and Consequential Damages Waiver), 11 (License), 12 (Ownership), 13 (Force Majeure), 14 (Applicable Law and Jurisdiction), 15 (Export Control), **Error! Reference source not found.** (Inventory eview), 19 (Notices),
28. **Survival.** Sections 5 (Payment), 7 (Term and Termination), 8 (Confidentiality), 9 (Warranty), 10 (Limitation of Liability and Consequential Damages Waiver), 11 (License), 12 (Ownership), 13 (Force Majeure), 14 (Applicable Law and Jurisdiction), 15 (Export Control), 18 (Inventory Review), 19 (Notices), 20 (Entire Agreement), 21 (No Waiver), 22 (Severability), 23 (Attorneys' Fees), 24 (No Agency), 27 (Survival), and the Glossary of Terms shall survive the termination or expiration of this Agreement."

Exhibit A
Glossary of Terms

In addition to the Definitions set forth in the WSCA Master Agreement, the following definitions shall apply to this Services Agreement:

Additional Services means installation of new Hardware, system additions, Hardware upgrades, dispatch of a field engineer, or non-mandatory engineering changes otherwise within the scope of the WSCA Master Agreement.

Advance Replacement means shipment of replacement Field-Replaceable Unit (FRU) before receiving failed or defective FRU.

Advanced Services means the proactive Services within the scope of the WSCA Master Agreement, and as set forth in the AS Service Description(s) found at http://www.cisco.com/go/servicedescriptions throughout the term of the agreement and/or SOW(s) selected by the Customer. Advanced Services does not include Cisco's core maintenance services, such as SMARTnet or Software Application Services, nor does it apply to the purchase, support, or maintenance of any Products.

Advanced Services Engineer means the Cisco engineer appointed to be the main point of contact for a Customer purchasing Advanced Services.

Application Software means non-resident or standalone Software Products listed on the Price List and within the scope of the WSCA Master Agreement, that include but are not limited to Cisco Systems® Network management Software, security Software, IP telephony Software, Internet appliance Software, Cisco® Intelligent Contact Management Software, IP Contact Center Software, and Cisco Customer Interaction Suite Software.

Business Days means the generally accepted days of operation per week within the relevant region where the Services shall be performed, excluding local holidays as observed by Cisco.

Cisco.com (http://www.cisco.com) is the Cisco website for its suite of online services and information.

Confidential Information means proprietary and confidential Information received by Cisco or Customer in connection with the Agreement and their relationship. Such Confidential Information may include, but is not limited to, trade secrets, know how, inventions, techniques, processes, programs, schematics, Software source documents, data, Customer lists, financial information, and sales and marketing plans or information which the receiving party knows or has reason to know is confidential, proprietary, or trade secret information of the disclosing party, as well as, in the case of Cisco, any information posted on Cisco.com.

Customer as defined in the WSCA Master Agreement means the entity purchasing Services for its own internal use either directly or through a Fulfilment Partner.

Data Collection Tools means Hardware or Software tools that support Cisco's ability to provide troubleshooting on critical cases, data analysis, and report-generation capabilities.

Depot Time or Local Time means Central European Time for Services provided in Europe-Middle-East and Africa, Australia's Eastern Standard Time for Services provided in Australia, Japan's Standard Time for Services provided in Japan, and Pacific Standard Time for Services provided in all other locations.

Deliverable means, with respect to each SOW, the items specified as deliverables in the SOW.

Device Type means a Cisco supported Hardware Product (for example, Cisco Catalyst® 6509 Switch, GSR 12000, and Cisco 7200 Series Router).

Direct Purchases means purchases of Services by Customer directly from Cisco.

Documentation is user manuals, training materials, Product descriptions and specifications, technical manuals, license agreements, supporting materials, and other information relating to Products or Services offered by Cisco, whether distributed in print, electronic, CD-ROM, or video format.

Equipment List means the list of Hardware and/or Software for which Cisco provides services.

Event means notification by Customer of its performance of a planned Network Hardware, Software, or configuration change.

Feature Set Upgrade means a separately licensed and priced Software release that contains an enhanced configuration or feature set.

Field-Replaceable Unit (FRU) means any component or subassembly of an item or unit of Hardware that reasonably can be replaced at Customer's location. FRUs also may be subject to size and weight limitations.

Four-hour Response means:

(i) For Advance Replacement Service, the four-hour time period commences upon the Cisco problem diagnosis and determination that a FRU is required and ends when the FRU is delivered onsite.

(ii) For onsite service, the four-hour time period commences upon the Cisco problem diagnosis and determination that remedial onsite service is required and ends when Cisco personnel arrive onsite.

Fulfilment Partner means a system integrator, distributor or reseller authorized by Cisco to sell Services under the WSCA Master Agreement in a Participating State.

Hardware means tangible Cisco equipment, devices, or components made available to Customers.

Indirect Purchases means purchases of Services by Customer through a Fulfilment Partner.

Intellectual Property means any and all tangible and intangible: (i) rights associated with works of authorship throughout the world, including but not limited to copyrights, neighboring rights, moral rights, and mask works, and all derivative works thereof, (ii) trademark and trade name rights and similar rights, (iii) trade secret rights, (iv) patents, designs, algorithms, and other industrial property rights, (v) all other intellectual and industrial property rights (of every kind and nature throughout the world and however designated) whether arising by operation of law, contract, license, or otherwise, and (vi) all registrations, initial applications, renewals, extensions, continuations, divisions, or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

Level 1 means support that is defined as having the necessary technical staff (Cisco or Cisco-authorized Reseller) with appropriate skill, perform installations, Remedial Hardware Maintenance, and basic Hardware and Software configuration on Cisco Products.

Level 2 means support that is defined as having the necessary technical staff with the appropriate skills to perform isolation, replication, and diagnosis of Internet-based problems on Cisco Product(s). Customer shall not report Software bugs to Cisco prior to attempting to identify the source of such bugs and testing in Customer's Network where appropriate. If the Customer cannot duplicate the bug in Customer's Network, Customer and Cisco shall cooperate in attempting to replicate and resolve related Software bugs in either Customer's or Cisco's test facility as mutually agreed. In all cases Customer will address Software bugs on a best effort basis to replicate same in Customer's Network and document activity to Cisco before seeking further resolution with Cisco's participation.

Local Time means local time on Business Days.

Maintenance Release means an incremental Software release that provides maintenance fixes and may provide additional Software functions. Cisco designates Maintenance Releases as a change in the digits to the right of the tenths digit or of the hundredths digit of the Software version number [x.x.(x) or x.x.x.(x)].

Major Release means a release of Software that provides additional software functions. Cisco designates Major Releases as a change in the ones digit of the Software version number [(x).x.x].

Minor Release means an incremental release of Software that provides maintenance fixes and additional Software functions. Cisco designates Minor releases as a change in the tenths digit of the Software version number [x.(x).x].

Network means a set of interconnected and interworking Cisco supported Hardware and Software that is implemented, operated, and supported by Customer from a single Network Operations Center (NOC).

Network Infrastructure means your core transport and aggregation Network technology (for example, metro optical, ATM/Frame Relay, IP core, and Cisco security devices including, but not limited to, Firewall, IDS, and VPN3000).

Network Infrastructure Size means the total value of Products in Customer's Network based on the global list price of the Products that Customer has purchased.

Participating State means a member of WSCA authorized under state law to participate under this Agreement who subsequently executes a Participating Addendum, or any other state or Local Public Body authorized by the WSCA Contract Manager and Cisco to be a party to the resulting Agreement who subsequently executes a Participating Addendum.

Price List means the price list for services applicable in the country where the Services are ordered or delivered.

Product means both Cisco Hardware and/or Software which are generally available.

Purchase Order or P.O. means a written or electronic order from Customer to Cisco for the Services to be provided by Cisco under this Agreement.

Remedial Hardware Maintenance means diagnosis and onsite replacement of Hardware components with FRUs.

RMA means Return Material Authorization.

Services means one or more of the services options selected by the Customer in its Purchase Order and described at: http://www.cisco.com/go/servicedescriptions.

Services Descriptions mean the detailed descriptions of the Services purchased by Customer which are incorporated in the MSA by reference.

Software means the software programs licensed to Customer by Cisco along with copies, Updates, or Upgrades to those software programs.

Standard Business Hours means (i) 8:00 AM to 5:00 PM, Depot time, on Business Days for replacement of failed Products and (ii) 8:00 AM to 5:00 PM, Local Time at location of the respective Cisco TAC, on Business Days for case handling of TAC calls.

Statement of Work (SOW) means the documents agreed upon by the parties that define Services and deliverables to be provided.

TAC means the Cisco Technical Assistance Center.

Technical Support Services means Services that provide both essential proactive and reactive operation and maintenance support Services identified as Technical Support Services at http://www.cisco.com/go/servicedescriptions.

Technology Application means specific technologies including, but not limited to, content networking, broadband, and IP telephony that do not operate at the Network Infrastructure level.

Third Party Products means third party Hardware and/or software, and all upgrades thereto, that are designated by Cisco as required for:

(i) The operation of Application Software in conformance with Cisco applicable Application Software Documentation.

(ii) Cisco support of the Application Software.

Transactional Advanced Services means the project related or consultancy Services sold under a Statement of Work.

Two-hour Response means:

(i) For Advance Replacement, the two-hour time period commencing with Cisco's problem diagnosis and determination that a FRU is required and ending when the FRU is delivered onsite.

(ii) For onsite service, the two-hour time period commencing with our problem diagnosis and determination that remedial onsite service is required and ending when Cisco personnel arrive onsite.

Update means Cisco Software Maintenance Releases, Minor Releases, and Major Releases containing the same configuration or feature set as originally acquired, unless the Customer has upgraded the applicable Hardware or Software to a configuration or feature set other than what was originally acquired, and the applicable license fee for that upgrade has been paid. Updates do not include Feature Set Upgrades.

WSCA shall mean the WSCA NASPO Contracting Alliance (WSCA). WSCA is a cooperative group contracting consortium for state government departments, institutions, agencies, and political subdivisions (i.e., colleges, school districts, counties, cities, etc.). Rights and obligations under this contract are limited to those Participating States who execute a Participating Addendum with Cisco.

"WSCA Contract Manager" or "Contract Manager" shall mean the individual state member designated as the contract manager by WSCA, currently the State of Utah, as responsible for the legal maintenance and administration of the WSCA Master Agreement, notices, reports, and any other pertinent documentation or information.

"WSCA Master Agreement" (also referred to as "Agreement" or "Contract") shall mean the underlying purchasing agreement executed by and between WSCA-NASPO Cooperative Purchasing Organization LLC ("State"), and Cisco, as now or hereafter amended.

Acronyms

AAA	Authorization and Accounting
AC	Alternate Current
ACD	Automatic Call Distributor
ACE	Application Control Engine
ACL	Access Control List
ACNS	Application and Content Network System
ADA	AD Active
ADC	Application Delivery Controllers
AES	Advanced Encryption Standard
AM	Assurance Manager
AN	Access Network
AP	Access Point
API	Application Programming Interfaces
APM	Application Performance Monitoring
APT	Adaptive Persistent Threats
AS	Agreement and as Set
ASA	Adaptive Security Appliance
ASIC	Application Specific Integrated Circuits
ASR	And System Resiliency
AT	Advanced Technologies
ATA	Analog Telephone Adapter
ATAS	Analog Telephone Adapters
ATM	Automated Teller Machines
AVC	Application Visibility and Control
AX	Application Experience
BGP	Border Gateway Protocol
BYOD	Bring Your Own Device
CA	Conditional Access
CAN	Campus Area Network
CARE	Citizen Access Routing Enterprise
CBC	Cipher Block Chaining
CCIE	Cisco Certified Internetworking Experts
CD	CDC Documentation
CD-ROM	Compact Disc-Read Only Memory
CDN	Cisco Development Network
CDS	Content Delivery Systems
CE	Compliance
CEO	Cisco Employs
CIFS	Common Internet File System
CMO	Contracts Management Office
CO2	Carbon Dioxide
CORBA	Common Object Request Broker Architecture
CPT	Carrier Packet Transport
CRS	Carrier Routing System
CSE	Customer Success Engineering
CTI	Computer Telephony Integration
CTO	Computer Telephony
CUBE	Cisco Unified Border Element
CUPC	Cisco Unified Personal Communicator
CUVA	Cisco Unified Video Advantage
CUWL	Cisco Unified Workspace Licensing

CVAA	Communications and Video Accessibility Act
D&B	Dun and Bradstreet
DCB	Data Center Bridging
DCNM	Data Center Manager
DH	Diffie Helman
DHCP	Dynamic Host Configuration Protocol
DIR	Department of Information Resources
DMM	Data Mobility Manager
DMVPN	Dynamic Multipoint VPN
DNA	Dialed Number Analyzer
DNS	Domain Name System
DoD	Department of Defense
DOM	Device Object Model
DRE	Data Redundancy Elimination
DSS	Data Security Standard
DTLS	Datagram Transport Layer Security
DTP	Dynamic Trunking Protocol
DWDM	Dense Wavelength Division Multiplexing
ECC	Elliptic Curve Cryptography
EGP	Exterior Gateway Protocol
ESX	Elastic Sky X
eTOM	Enhanced Telecom Operations Map
ETSI	European Telecommunications Standards Institute
EULA	End User License Agreement
F.O.B	Freight On Board
FAR	Federal Acquisition Regulation
FC	Fibre Channel
FCC	Federal Communications Commission
FCIP	Fibre Channel Internet Protocol
FCOE	FIBRE CHANNEL OVER ETHERNET
FICON	Fibre Connection
FISMA	Federal Information Security Management Act
FPM	Flexible Packet Matching
FRU	Field Replaceable Unit
FY	Fiscal Year
GCM	Galois Counter Mode
GE	Gigabit Ethernet
GHz	Gigahertz
GLBA	Gramm Leach Bliley Act
GMPLS	Generalized Multiprotocol Label Switching
GPL	Global Price List
GRAMA	Government Records Access and Management Act
GSR	Gigabit Switch Router
GUI	Graphical User Interface
HA	High Availability
HCS	HOSTED COLLABORATION SOLUTIONS
HIPAA	Health Insurance Portability and Accountability Act
HP	Hewlett Packard
HTTP	Hyper Text Transport Protocol
HTTPS	HTTP Secure
HVAC	Heating Ventilating and Air Conditioning
I.E	Industrial Ethernet
I/O	Input/Output
IBM	International Business Machines

IBSG	Internet Business Solutions Group
ICA	Independent Computing Architecture
ID	In Different
IDS	Integrated Switch
IDSM	Intrusion Detection Services Module
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IF	Intermediate Frequency
IGP	Interior Gateway Protocol
IM	Instant Message
IME	Intercompany Media Engine
IOA	Input/output Acceleration
IOS	IOS Operating System
IP	Internet Protocol
IP/MPLS	Internet Protocol/ Multiprotocol Label Switching
IPICS	IP Interoperability and Collaboration System
IPoDWDM	Internet Protocol over Dense Wavelength Division Multiplexing
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
IPTV	Internet Protocol Television
IS	Intermediate System
ISAPI	Intelligent Services API
iSCSI	Internet Small Computer Systems Interface
ISE	Identity Services Engine
ISL	Inter Switch Link
ISM	INTERNAL SERVICE MODULE
ISO	International Standards Organization
ISP	Internet Service Providers
ISR	Integrated Services Routers
ISSU	In Service Software Upgrade
ISV	Independent Software Vendors
IT	Integrated Tools
ITIL	Information Technology Information Library
ITS	Intelligent Transportation System
ITU	International Telecommunications Union
IVR	Inter VSAN Routing
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LAN/WAN	Local Area Network/Wide Area Network
LCMT	Learning Credits Management Tool
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
LMS	LAN Management Solution
LUN	Logical Unit Numbers
MAC	Moves Adds and Changes
MACsec	MAC Security
MAN	Metro Area Networks
MAPI	Messaging API
MCS	MEDIA CONVERGENCE SERVERS
MD5	Message Digest 5
MDM	Mobile Data Management
MDS	Multilayer Directors
MoH	Music on Hold
MPLS	Multiprotocol Label Switching

MPLS-TP	Multi-Protocol Label Switching Transport Profile
MPPS	Million Packets per Second
MS	Microsoft
MSA	Master Services Agreement
MSE	Mobility Services Engine
MSPP	Multiservice Provisioning Platform
MSRP	Microsoft Remote Procedure
MSTP	Multiservice Transport Platform
MTTR	Mean Time to Resolution
NAC	Network Admission Control
NAM	Network Analysis Module
NASDAQ	National Association of Securities Dealers Automated Quotations
NAT	Network Address Translation
NBAR	Network Based Application Recognition
NBD	Next Business Day
NBI	Northbound Interface
NCS	Network Control System
NFP	Network Foundation Protection
NFS	Network File System
NGE	Next Generation Encryption
NGFW	Next Generation Firewalls
NGN	Next Generation Network
NIC	Network Interface Card
NO	Network Operations
NOC	Network Operations Center
NSA	National Security Agency
NTP	Network Time Protocol
OEM	Original Equipment Manufacturer
ONS	Optical Networking Switch
OPEX	Operating Expense
OS	Operating Systems
OSM	Original Storage Manufacturers
OTN	Optical Transport Network
OTS	Optical Transport System
OWA	Outlook Web Access
P.O.	Purchase Order
PBR	Policy Based Routing
PC	Phone Calling
PCI	Payment Card Industry
PDF	Portable Document Format
PE	Participating Entities
PIX	Private Internet Exchange
PM	Project Manager
PMC	Packet Mode Channel
PMP	Program Management Professional
PoE	Power the Endpoint
PRO	Planning and Reporting Officer
PTZ	Pan, Tilt, Zoom
PVRST	Per VLAN Rapid Spanning Tree
Q&A	Question and Answer
QoS	Quality of Service
R&D	Research and Development
RADIUS	Remote Authentication Dial-in User Service
RAN	Radio Access Network

RBAC	Role Based Access Control
REST	Representational State Transfer
RF	Radio Frequency
RFC	Request for Comment
RFID	Radio Frequency Identification
RFP	Request for Proposal
RFR	Return for Repair
RMA	Return Material Authorization
ROADM	Reconfigurable Optical Add Drop Multiplexer
ROI	Return on Investment
RSA	Rivest Shamir and Adleman
SAN	Storage Area Networks
SAP	Second Audio Program
SD	Standard Definition
SDH	Synchronous Digital Hierarchy
SDK	Software Development Kit
SDM	System Data Movers
SDN	Software Defined Networking
SET	Secure Electronic Transaction
SF	Small Form-Factor
SFP	Small Form-Factor Pluggable
SIEM	Security Information and Event Management
SIO	Security Intelligence Operations
SIP	SPA Interface Processors
SKU	Standard Known Unit
SLA	Service Level Agreement
SME	Storage Media Encryption
SMS	Short Message Service
SMTP	Simple Mail Transport Protocol
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SOW	Statement of Work
SOX	Sarbanes Oxley
SPA	Shared Port Adapters
SPI	Stateful Protocol Inspection
SQL	Structured Query Language
SRE	Services Ready Engines
SRST	Survivable Remote Site Telephony
SSL	Secure Sockets Layer
TAC	Technical Assistance Center
TACACS	Terminal Access Controller Access Control System
TBD	To Be Determined
TCO	Total Cost of Ownership
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TFO	Transport Flow Optimization
TIA	Telecommunications Industry Association
TLS	Transport Layer Security
TP	Transport Profile
U.S.	United States
UC	Unified Communications
UCS	Unified Computing System
UCSS	Unified Communications Software Subscription
UL	Underwriters Laboratories

URL	Uniform Resource Locators
US	United States
USD	Unified Service Delivery
UTM	Unified Threat Management
VDC	Virtual Device Context
VDI	Virtual Desktop Infrastructure
VLAN	Virtual Local Area Networks
VM	Virtual Machine
VNI	Visual Networking Index
VNMC	Virtual Network Management Center
VoD	Video on Demand
VoIP	Voice over Internet Protocol
VP	Virtual Packet
VPLS	Virtual Private LAN Service
VPN	Virtual Private Networking
VRRP	Virtual Router Redundancy Protocol
VSAN	Virtual SAN
VSG	Virtual Security Gateway
VSM	Virtual Supervisor Module
VSS	Virtual Switching System
VXI	Virtual Experience Infrastructure
W3C	World Wide Web Consortium
WAAS	Wide Area Application Services
WAE	Wide Area Application Engine
WAN	Wide Area Networks
WAVE	Wide Area Virtualization Engine
WCAG	Web Content Accessibility Guidelines
WIDS	Wireless Intrusion Detection System
WIPS	Wireless Intrusion Prevention System
WLAN	Wireless LAN
WSCA	Western States Contracting Agreement
WSON	Wavelength Switched Optical Network
XML	Extensible Markup Language