

REQUEST FOR QUOTATION
11-162

All Offerors must have and maintain a current State Term
Schedule Contract with the Department of Administrative Services

DATE ISSUED: June 17, 2010

The state of Ohio, through the Ohio Department of Public Safety
Administration Division is requesting a quotation for:

Technical Training for Mainframe Resources

YOU ARE INVITED TO SUBMIT A QUOTATION FOR THE PRODUCT DESCRIBED IN THIS
DOCUMENT. SIGNED QUOTATION MUST ARRIVE BY 3:00 P.M. JULY 6, 2010, TO:

MARK A. CONTOSTA, CPPO, CPPB
CHIEF, PURCHASING
OHIO DEPARTMENT OF PUBLIC SAFETY
1970 W. BROAD ST., 5TH FLOOR
P.O. BOX 182081
COLUMBUS, OH 43218-2081

FAX QUOTATION TO:

MARK A. CONTOSTA, CPPO, CPPB
CHIEF, PURCHASING
OHIO DEPARTMENT OF PUBLIC SAFETY
614-752-7823 (fax)
614-752-4225

FAXED QUOTATION TO BE FOLLOWED BY ORIGINAL NO LATER THAN JULY 13, 2010 TO:

MARK A. CONTOSTA, CPPO, CPPB
CHIEF, PURCHASING
OHIO DEPARTMENT OF PUBLIC SAFETY
1970 W. BROAD ST., 5TH FLOOR
P.O. BOX 182081
COLUMBUS, OH 43218-2081

1 General Overview

1.1 Purpose:

The Ohio Department of Public Safety (ODPS) is soliciting quotations from Offerors to provide Computer Technology Industry Association (CompTIA) A+ and Network+ certifications courses to prepare participants to successfully transition support from the Unisys mainframe computer to a Windows server environment. At the conclusion of the training, the participants shall be prepared to pass the CompTIA A+ and Network+ certification examinations. The participants are not required to the CompTIA certification exams and testing is not part of this Contract. However, the Offeror must provide the participants the opportunity to take the CompTIA certification examination(s) immediately following their successful completion of the courses, coordinated by and at the participants' expense.

This project requires the Contractor to provide appropriate facilities, training materials, and qualified instruction for specific technical training courses for twenty (20) individuals. Participants will attend Training in groups of ten (10) individuals. The training shall consist of courses covering the curriculum established by CompTIA for the successful completion of the A+ and Network+ certification examinations. CompTIA is the organization responsible for oversight and administration of the A+ and Network+ certification examinations (Supplements One, Two and Three detail the required CompTIA objectives).

Throughout this document, the term "Training" will refer to the training, materials and facilities to be supplied by the Contractor. "Participant(s)" will refer to all the ODPS employees identified as taking part in the Training.

If a suitable offer is made in response to this RFQ, the state of Ohio ("State") may enter into a contract (the "Contract") to have the selected Offeror (the "Contractor") perform the Work (described in the General Overview and Scope of Work). This RFQ provides details on what is required to submit a quotation for the Work, how the State will evaluate the quotations, and what will be required of the contractor in performing the Work.

Once awarded, the term of the Contract will be from the award date through June 30, 2011. This Contract may be extended by mutual agreement between the ODPS and the Contractor for one (1) additional year, at the Offered Rate, subject to and contingent upon the discretionary decision of the Ohio General Assembly to appropriate funds for this Contract in the new biennium. The awarded Contractor must maintain a valid State Term Schedule (STS) Contract for the length of this contract.

This RFQ also provides the estimated dates for the various events in the submission process, selection process, and performance of the work. While these dates are subject to change, prospective Offerors must be prepared to meet them as they currently stand. Any failure to meet a deadline in the submission or evaluation phases and any objection to the dates for performance in the work phase may result in the State refusing to consider the quotation of the Offeror.

1.2 Background:

Currently, the ODPS is involved in an effort to migrate all of the applications, data, and functionality from the Unisys mainframe computer to a Windows server environment. The changes in technology resulting from this effort require the employees involved to undergo training that will enable them to continue to contribute effectively and productively in this new environment.

1.2.1 The following environments/applications run on the mainframe:

1.2.1.1 Pacbase is the development tool for the Driver License and Vehicle Registration systems.

1.2.1.2 Enterprise Application Environment (EAE), formerly called Logic and Information Network Compiler (LINC), a Unisys proprietary language, is used for the Withdrawal Management System (used for driver license suspension management) and Transaction Database (used as a financial transaction repository).

1.2.1.3 The remaining applications residing on the mainframe consist of straight Common Business-Oriented Language (COBOL) programs and a multitude of interfaces with non-mainframe applications, such as the Law Enforcement Automated Data System (LEADS).

1.2.2 The migration from the mainframe to a Windows server environment will occur in two (2) phases:

1.2.2.1 Phase 1 is migrating off the mainframe. The instituted solution involves purchasing tools required to enable native code (Pacbase, and, in the case of EAE, the next generation replacement called Agile Business Suite) to be compiled in a format operable in a Windows environment. This includes purchasing the compiling tools, establishing the environments, transitioning databases to Structured Query Language (SQL) Server, and providing the developers with the necessary training. Both Pacbase and Agile Business Suite have developed plans for moving applications in efficient, methodological, and risk-mitigating phases.

1.2.2.2 Phase 2 includes the transition of the compiled applications and programs to a modern architecture utilizing .NET technologies. Pacbase and Agile Business Suite will no longer be used for development, and the business rules will be written in C# Programming with the latest version of the .Net Framework.

1.2.3 Targeted Group for Training:

The group targeted to successfully complete the training outlined in this document are the ODPS resources currently tasked with the support of the Unisys mainframe. Since the applications will move from the mainframe to a Windows, server-based environment, the ODPS determined courses designed to cover the objectives supplied by CompTIA for the A+ and Network+ certification examinations will adequately prepare these resources to continue to contribute once the mainframe is decommissioned.

1.2.4 Optional Certification(s) Testing (at the participant's expense):

The certifications are not considered mandatory for any ODPS participants. Participants may elect to pursue these certifications. The Offeror must provide the required testing facilities and requirements.

1.2.4.1 CompTIA A+ certification requires a candidate must pass two exams:

1.2.4.1.1 CompTIA A+ Essentials, exam code 220-701, measures the necessary competencies of an entry-level IT professional. It tests for the fundamentals of computer technology, networking and security, as well as the communication skills and professionalism now required of all entry-level IT professionals.

1.2.4.1.2 CompTIA A+ Practical Application, exam code 220-702, measures the necessary competencies of computer support technicians including competence in areas such as installation, preventative maintenance, networking, security and troubleshooting

1.2.4.2 CompTIA Network+, exam code BR0-002, measures a technician's competency in managing, maintaining, troubleshooting, installing and configuring basic network infrastructure.

2 Specifications:

2.1 Scope of Work:

The ODPS is seeking the services of a Contractor to provide appropriate facilities, training materials, and qualified instruction for specific technical training courses for twenty (20) individuals. For all courses, participants will attend Training in two (2) groups of ten (10) individuals.

2.1.1 Curriculum: The Contractor will provide a detailed curriculum for the proposed CompTIA A+ and Network+ courses. These curricula will map directly to the learning objectives listed by CompTIA as material covered in the certification exams.

The Offeror must submit the proposed detailed curriculum with their quotation. The ODPS will review and approve the final curriculum proposed by the Offeror.

- 2.1.2 **Assessments:** The Contractor will provide assessments for each course for all Participants. The purpose of the assessment process is to capture the progress of each Participant through the Training.

The Offeror must submit the proposed assessment plan with their quotation. The ODPS will review and approve the final assessment process proposed by the Offeror.

- 2.1.3 **Instructional Materials:** The Contractor will supply all training materials appropriate for each course.

The Offeror must submit a detailed list of instructional materials for each course with their quotation. The ODPS will review and approve the final instructional materials proposed by the Offeror.

- 2.1.4 **Retraining:** The Contractor must allow participants to re-take course(s) at no additional cost, up to twelve (12) months after conclusion of all training.

The Offeror must include a narrative in their Cover Letter indicating the participants will be able to re-take the course(s) at no additional cost to the state of Ohio.

- 2.1.5 **Additional Participants:** The ODPS reserves the right to add participants to the training sessions at the offered rate.

The Offeror must include a statement in their Cover Letter indicating the ODPS may add participants to the training sessions at the offered rate.

- 2.1.6 **Examinations:** The Contractor must provide the participants the option to take the CompTIA certification examination(s) immediately following their successful completion of the courses.

The certification exam is not mandatory for the class participants. Each participant will be responsible for the procurement and scheduling of exams.

The Offeror must submit detailed testing and registration procedures for each exam with their quotation. The procedures, at a minimum, must include the following: contact person(s); schedule requirements; and payment methods accepted by the Offeror.

- 2.1.7 **Scheduling:** The Contractor must provide these courses and optional testing within the following time frame:

Week	Training Course	Group
1	CompTIA A+	1
2		
3	CompTIA A+	2
4	CompTIA Network+	1
5		
6	CompTIA Network+	2

- 2.1.8 **Facilities:** All courses are to be held at a location within Franklin County, Ohio that is reasonably accessible to the Participants. The location must contain appropriate facilities for conducting the training courses and taking the certification examinations. This will include, but not be limited to, computers loaded with the appropriate software, both for the participants and the instructor(s).

The Offeror must submit a description of the proposed training site (i.e. classroom size, training equipment) and detail how the Offeror's proposed training site accommodates the optional participant testing.

2.2 Mandatory Offeror Requirement:

The Offeror must meet the following minimum qualification for further consideration:

2.2.1 The Offeror must have the appropriate facilities, located within Franklin County, Ohio and the equipment to facilitate training of participants and allow participants to take the CompTIA certification exams onsite, immediately following the completion of each course.

2.3 Mandatory Instructor (Consultant/Resource) Requirements and Qualifications:

The offered instructor for each course must meet the following minimum qualifications for further consideration:

2.3.1 Five (5) years of technical instruction experience, with a minimum of three (3) years in CompTIA A+ and Network+ certification preparation.

2.3.2 Five (5) years of hands-on work experience involving tasks (See Supplement One, Two, and Three) associated with the objectives identified by CompTIA as required knowledge for the A+ and Network+ certification examinations.

The ODPS will review and approve the curriculum, instructional materials, and instructor resume prior to each course.

The proposed Consultant/Resource must demonstrate the following requirements in order to be eligible for further consideration:

2.3.3 Must have excellent oral and written skills and possess strong meeting and work session facilitation skills.

2.3.4 Must have excellent organizational skills, proven analytical, planning, problem solving, and decision-making skills.

2.3.5 Must be knowledgeable in the English language and speak clearly and understandably using the English language.

During the interview process with the ODPS staff, the resource consultant(s) must demonstrate competence/experience in their specific area(s) of project assignment. The resource's experience must also be documented for review and verification. Offered resources not showing technical or functional competency/experience will be reason to reject the Offeror's proposal. It is the responsibility of the Offeror to pre-screen their candidates to ensure compliance.

2.4 Deliverables:

2.4.1 Instructional Materials: The Contractor will supply all ODPS approved training materials appropriate for each course. A detailed list of instructional materials for each course is to be included in the Offeror proposal.

2.4.2 Provide a five (5) day course covering all the objectives indicated by CompTIA as part of the 220-701 and 220-702 A+ certification exams (See Supplements One, Two, and Three detail the CompTIA objectives).

2.4.2.1 Possess the facilities/equipment enabling the participant, based on successful completion of the course defined in 2.4.2, to take the 220-701 and 220-702 certification examinations immediately upon completion of the course and in the same facility as the course was provided.

2.4.3 Provide a five (5) day course covering all the objectives indicated by CompTIA as part of the Network+ certification exam.

2.4.3.1 Possess the facilities /equipment enabling the participant, based on successful completion of the course defined in 2.4.3, to take the Network+ certification examination, exam code BR0-002, immediately upon completion of the course and in the same facility as the course was provided.

2.4.4 Assessments: The Contractor will provide assessments for each course for all Participants. The purpose of the assessment process is to capture the progress of each Participant as he/she progresses through the Training.

2.4.4.1 The ODPS will review and approve the assessment process proposed by the Contractor.

2.4.5 Retraining: The Contractor must allow participants to re-take courses at no additional cost, up to twelve (12) months after conclusion of all training.

2.5 The ODPS State Work Support Requirements:

2.5.1 The following items will be provided to the selected Offeror by the ODPS point of contact as determined by the Offeror's quotation.

2.5.1.1 Any reasonable request for access to the ODPS places of business.

2.5.1.2 Help in setting up interview access with the ODPS personnel.

2.5.2 The Offeror must describe the support it wants from the State to accomplish the project other than what the State has offered elsewhere in this Scope of Work. Specifically, the Offeror must address the following:

2.5.2.1 Nature and extent of State support required;

2.5.2.2 Assistance from State staff and the experience/qualification level required; and

2.5.2.3 Other support requirements.

2.5.3 The State may not be able or willing to provide the additional support the Offeror lists in this part of its RFQ response. The Offeror must therefore indicate whether its request for additional support is a requirement for its performance. If any part of the list is a requirement, the State may reject the Offeror's response if the State is unwilling or unable to meet the requirements.

2.6 Estimated Schedule:

RFQ Release	June 17, 2010
Inquiry Period Begins	June 18, 2010
Inquiry Period Ends	July 2, 2010
RFQ opening	July 6, 2010 at 3:00 p.m. EDT
Evaluations / Interviews Conducted	July 7, 2010 thru July 16, 2010
Selection of Contractor/Approval Package to DAS	July 19, 2010
DAS approval and sanction of Award	July 22, 2010
Anticipated Award Date	July 26, 2010
Proposed Training Start Date	September, 2010

3 Terms and Conditions:

3.1 Contractual Obligations:

The terms and conditions for the services to be performed are in accordance with the contractual obligations established by the ODPS.

3.2 Contract Term:

Once awarded, the term of the Contract will be from the award date through June 30, 2011. This Contract may be extended by mutual agreement between the ODPS and the Contractor, at the Offered Rate, subject to and contingent upon the discretionary decision of the Ohio General Assembly to appropriate funds for this Contract in the new biennium.

3.3 Contract Renewal:

The ODPS may renew this agreement by giving sixty (60) days written notice prior to the expiration, for an additional six (6), one (1) month extensions at the Offered hourly rate not to exceed the current contract rate.

3.4 Compensation:

The Contractor will not submit more than one invoice for work performed within a 30-day period. In order to be considered a proper invoice, the Contractor shall include on all invoices the proper vendor identification number, purchase order number, and total cost of services; and submit an original and three copies monthly to:

Ohio Department of Public Safety
Attn: Fiscal Services (BMV)
P.O. Box 16520
Columbus, Ohio 43216-6520

3.5 Sub-contracting:

Sub-contracting will be allowed only with prior written approval from the ODPS.

3.6 Background Check:

A background check, at the ODPS expense, may be performed on the designated contact person for assignment to this Agreement. The designated contact person may be required to complete a "Background Information Form" furnished by the ODPS. Failure to pass the background check will result in immediate dismissal of the resource, whereupon, the Offeror must submit a replacement resource with equal or better qualifications within the time limits as set forth in 3.7 Replacement Personnel of this RFQ (See Attachment 10, Background Check Form).

3.7 Replacement Personnel:

The quality and professional credentials of the proposed resource(s) submitted in the Offeror's quotation are material factors in the State's decision. The Contractor may not remove the proposed resource(s) from the Work without the prior, written consent of the State, for the duration of the Contract, including any extensions except for reasons listed. If the Contractor removes the proposed resource(s) without prior written consent of the State, the Contractor will be in default and the State may terminate this Contract immediately for cause and without any cure period.

The Contractor may only remove the proposed resource(s) listed in the quotation response for legal or disciplinary reasons. In this event, the Contractor will have seven (7) business days to provide two (2) proposed qualified replacement resource(s) for each removed resource. The State may reject the proposed replacement resource(s) for the following reasons:

- 3.7.1 Failure of the resource(s) to meet the Mandatory Requirements and Qualifications identified in this RFQ.
- 3.7.2 Failure of the Contractor to provide two (2) qualified replacement resources for each removed resource.

If the State rejects the replacement resource(s), the Contractor will be in default and the State may terminate this Contract immediately for cause and without any cure period.

3.8 Declaration Regarding Material Assistance/NonAssistance to Terrorist Organization - Sec. 2909.33 (C):

In accordance with R.C. 2909.33(C), I certify that I meet one of the following conditions:

3.8.1 I have not received, nor will receive as a result of this contract, an aggregate amount greater than one hundred thousand dollars (\$100,000) in business or funding, excluding personal benefits, from the state, instrumentalities, or political subdivisions during the current fiscal year;

or

3.8.2 I have received, or will receive as a result of this contract, an aggregate amount greater than one hundred thousand dollars (\$100,000) in business or funding, excluding personal benefits, from the state, instrumentalities, or political subdivisions during the current fiscal year.

and,

I have either pre-certified with the Office of Budget and Management, or have completed the Declaration of Material Assistance form certifying that I have not provided material assistance to any organization on the Terrorist Exclusion List, as that term is defined in R.C. 2909.21.

<http://www.publicsafety.ohio.gov/links/HLS0038.pdf>

3.9 Nondisclosure Agreement:

Contractors/Consultants may be required to submit a completed and signed Nondisclosure Agreement to the ODPS as soon as possible after the Contractor has been accepted following the interview process but prior to a Purchase Order being issued. If required, failure to provide the required form may result in immediate dismissal of the resource, whereupon, the Offeror must submit a replacement resource with equal or better qualifications within the time limits as set forth in 3.7 Replacement Personnel of this RFQ (See Attachment 11, Nondisclosure Agreement).

3.10 Confidentiality and Conduct Agreement:

Contractors/Consultants may be required to submit a completed and signed Confidentiality and Conduct Agreement to the ODPS as soon as possible after the Contractor has been accepted following the interview process but prior to a Purchase Order being issued. Failure to provide the required form may result in immediate dismissal of the resource, whereupon, the Offeror must submit a replacement resource with equal or better qualifications within the time limits as set forth in 3.7 Replacement Personnel of this RFQ (See Attachment 12, Confidentiality and Conduct Agreement).

3.11 Work Rules, Policies and Procedure Compliance:

The Contractor agrees, as a condition of being awarded this contract, to require each of its agents, officers, and employees to abide by the state of Ohio and the Ohio Department of Public Safety's policies, work rules, safety rules, or policies regulating the conduct of persons on State property at all times while performing duties pursuant to this contract. Additionally, if the Contractor is using or possessing State data or accessing State networks and systems, the Contractor must comply with all applicable State rules, policies and regulations regarding data security and integrity. And when on any property owned or controlled by the State, the Contractor must comply with all security and safety rules, regulations, and policies applicable to people on those premises. The Contractor agrees and understands that a violation of any of these policies or rules constitutes a breach of the contract and sufficient grounds for immediate termination of the contract by the Ohio Department of Public Safety. The Contractor's resources assigned to work on this project will be provided a copy of the Consultant Policy Assignments and are required to sign a verification of receipt and acceptance/compliance within five (5) business days after start of work onsite at the ODPS.

3.12 Equal Opportunity Requirements:

- 3.12.1 The Contractor, and any of its subcontractors, shall comply with the requirements under ORC § 125.111. The Contractor and any of its subcontractors shall not discriminate against anyone because of race, color, religion, creed, sex, age, disability, national origin or ancestry.
- 3.12.2 The Contractor certifies that both the Contractor and any of its subcontractors are in compliance with all applicable federal and state laws, as well as rules and regulations governing fair labor and employment practices.
- 3.12.3 The ODPS encourages both the Contractor and any of its subcontractors to purchase goods and services from certified Minority Business Enterprise (MBE) and Encouraging Diversity Growth and Equity (EDGE) vendors.

4 Submission of Quotations and Additional Offeror Responsibilities:**4.1 Inquiries:**

Offerors may make inquiries regarding this RFQ any time during the inquiry period listed in Section 2.6, Estimated Schedule. To make an inquiry, Offerors must use the following process:

- 4.1.1 Access the State Procurement Web site at <http://www.ohio.gov/procure>;
- 4.1.2 From the Navigation Bar on the left, select "Find It Fast";
- 4.1.3 Select "Doc/Bid/Schedule #" as the Type;
- 4.1.4 Enter "ODPS" and the RFQ Number found on Page 1 of the document;
- 4.1.5 Click "Find It Fast";
- 4.1.6 On the document information page, click "Submit Inquiry";
- 4.1.7 On the document inquiry page, complete the required "Personal Information" section by providing:
 - 4.1.7.1 First and last name of the prospective Offeror's representative who is responsible for the inquiry;
 - 4.1.7.2 Name of the prospective Offeror;
 - 4.1.7.3 Representative's business phone number; and
 - 4.1.7.4 Representative's e-mail address.
- 4.1.8 Type the inquiry in the space provided including:
 - 4.1.9 A reference to the relevant part of this RFQ;
 - 4.1.10 The heading for the provision under question; and
 - 4.1.11 The page number of the RFQ where the provision can be found.
- 4.1.12 Click "Submit".
- 4.1.13 Offerors submitting inquiries will receive an immediate acknowledgement that their inquiry has been received as well as an e-mail acknowledging receipt. Offerors will not receive a personalized e-mail response to their question, nor will they receive notification when the question has been answered.
- 4.1.14 Offerors may view inquiries and responses using the following process:
 - 4.1.14.1 Access the State Procurement Web site at <http://www.ohio.gov/procure>;
 - 4.1.14.2 From the Navigation Bar on the left, select "Find It Fast";
 - 4.1.14.3 Select "Doc/Bid/Schedule #" as the Type;

4.1.14.4 Enter "ODPS" and the RFQ Number found on Page 1 of the document;

4.1.14.5 Click "Find It Fast";

4.1.14.6 On the document information page, click the "View Q & A" button to display all inquiries with responses submitted to date.

4.1.15 The State will try to respond to all inquiries within forty-eight (48) hours of receipt, excluding weekends and State holidays. The State will not respond to any inquiries received after 8:00 a.m. on the inquiry end date.

4.1.16 When an amendment to this RFQ is necessary less than four (4) days before the RFQ due date, the State may extend the RFQ due date through an announcement. Amendment announcements may be provided any time before 4:00 p.m. on July 2, 2010.

4.2 Requests for Previous Quotations/Contracts:

Requests from potential Offerors for copies of previous RFQ's, past Offeror quotations, or contracts for any potentially related projects, are Public Records Requests (PRRs) and not clarification questions regarding the present RFQ. PRRs should be submitted by e-mail to PublicRecords@dps.state.oh.us or mail to:

Ohio Department of Public Safety Public Records Manager/Administrator Administration Division 1970 W. Broad Street Columbus, Ohio 43223

The posted time frames for responses to internet questions for RFQ clarification do not apply PRRs. The ODPS does not guarantee that a response to a PRR will be made within the time frame controlling this RFQ. Any failure or delay of the ODPS in responding to the PRR will have no bearing on the deadlines found in this RFQ.

4.3 Clarifications:

4.3.1 The ODPS may request clarifications on quotations to ensure the quotations are understood by the ODPS.

4.3.2 Clarifications shall be requested using e-mail to an address specified in the RFQ response, and clarifications shall be sent to the ODPS as a "reply" to the request for clarification within twenty-four (24) hours (not including weekends or holidays).

4.4 Intentions:

4.4.1 It is the intent of the State to describe a complete set of requirements. Any incidental items omitted from these specifications but needed to satisfactorily complete the requirements, must be provided by the Offeror and will be included in the quotation.

4.4.2 If the State decides to revise this RFQ before the response due date, addenda will be posted to the Ohio Business Gateway:

<http://www.ohio.gov/procure>

4.4.3 Quotations must be received no later than 3:00 P.M., July 6, 2010 Quotations should be:

Mailed to:	Delivered to:
Mark A. Contosta, CPPO, CPPB Chief, Purchasing Ohio Department of Public Safety 1970 W. Broad St., 5 th floor P.O. Box 182081 Columbus, Ohio 43218-2081	Mark A. Contosta, CPPO, CPPB Chief, Purchasing Ohio Department of Public Safety 1970 W. Broad St., 5 th floor Columbus, Ohio 43223

DELIVERY INSTRUCTIONS

Quotations, whether delivered through U.S.P.S., UPS, FedEx or by hand to the ODPS must be complete, cover page of the original quotation signed in blue ink, envelope sealed with the RFQ number and title clearly marked on the outside of the envelope or box.

If delivering quotation in person to the ODPS, come to the loading docks on the South side of the building. There is a door to the immediate right of the right most loading bay. Next to the door is a bell to ring for service. Deliver the quotation to the ODPS mail room. Make sure the time and date of delivery is noted on the quotation and logged by the person receiving the envelope. If any problems are encountered, in the delivery, and to verify receipt of the quotation call J.S. McCasland at (614) 752-2052. Attempts to deliver to the Highway Patrol Officer at the front desk of the Customer Service Center, as in the past, will be refused. The quotations will be received between the hours of 8:00 A.M. and 4:00 P.M. (3:00 P.M. on July 6, 2010) Monday through Friday.

- 4.4.4 Upon receipt by the ODPS Purchasing, all quotations will be time and date stamped. Postmarks or other times/dates appearing on the quotation envelope will not be considered as the official time/date of receipt. An RFQ response submitted with insufficient postage or C.O.D. will not be accepted.
- 4.4.5 A facsimile of an offer will be considered, but an originally signed copy (signature to be in Blue Ink) of the offer must be received within seven (7) days after the quotation opening. Any other mode of transmitting a quotation to the ODPS shall not be considered a valid quotation.

4.5 Mandatory Content of RFQ Response:**4.5.1 RFQ Response Cover Letter:**

The Offeror must **HAND SIGN AND DATE THE RFQ COVER LETTER IN BLUE INK** before submitting the quotation. The RFQ cover letter shall be on company letterhead, with an original signature in Blue Ink, and include the following:

- 4.5.1.1 A statement indicating participants will be able to re-take the course(s) at no additional cost to the state of Ohio for a period of one (1) year following the completion of training (Section 2.1.4);
- 4.5.1.2 A statement indicating the ODPS may add participants to the training sessions at the offered rate (Section 2.1.5);
- 4.5.1.3 The Proposed Instructor; and
- 4.5.1.4 The Total Not-to-Exceed Fixed Cost of the submitted quotation.

4.5.2 Quotation /Cost Summary:

Offerors will complete the Quotation/Cost Summary form/table found in Attachment 1 and identify all resources and costs associated with performing the work. The ODPS is expecting the rates quoted will be significantly discounted from the State Term Schedule (STS) rates. The Offeror will provide and attach a comparison of their approved STS rates and the discounted rates included in the RFQ response.

Offerors may not reformat these forms. Each Offeror must complete the Cost Summary forms in the exact format provided. Any reformatting may cause the State to reject the Offeror's quotation.

These forms and associated instructions are what the State projects as the final Cost Summary forms at the present time. The State reserves the right to modify the Cost Summary forms and instructions at the time qualified Offerors are invited to submit their not-to-exceed fixed price quotation. Completed Cost Table forms are to be provided when the quotations are submitted.

Offerors are to copy as many forms as are needed, and page number each sheet in the upper right hand corner. If there is any doubt as to which page a particular item should be recorded under, Offerors are to use their discretion. The important thing is that the item is listed and accounted for, not particularly where it is listed so that all costs are identified. The dollar amounts listed by the Offerors must represent a NOT-TO-EXCEED FIXED PRICE.

The State will not be liable for any costs the Offeror does not identify in its response to this RFQ (Attachment 1) and the Offeror must identify all costs associated with performing the work. The ODPS is expecting the hourly rates quoted shall be significantly discounted from the STS rates. The Offeror will provide and attach a comparison of their approved STS rates and the discounted rates included in the RFQ response.

4.5.3 Curriculum:

The Offeror must submit the proposed detailed curriculum with their quotation. The ODPS will review and approve the final curriculum proposed by the Offeror.

4.5.4 Assessments:

The Offeror must submit the proposed assessment plan with their quotation. The ODPS will review and approve the final assessment process proposed by the Offeror.

4.5.5 Instructional Materials:

The Offeror must submit a detailed list of instructional materials for each course with their quotation. The ODPS will review and approve the final instructional materials proposed by the Offeror.

4.5.6 Examinations:

The Offeror must submit detailed testing and registration procedures for each exam with their quotation. The procedures, at a minimum, must include the following: contact person(s); schedule requirements; and payment methods accepted.

4.5.7 Scheduling:

The Offeror must submit a Schedule detailing the proposed time frame for each course and optional testing.

4.5.8 Facilities:

The Offeror must submit a description of the proposed training site (i.e. classroom size, training equipment) and detail how the Offeror's proposed training site accommodates the optional participant testing.

4.5.9 Mandatory Instructor (Consultant/Resource) and Qualifications / Personnel Profile Summaries:

The Offeror shall detail the Offeror and proposed resource(s) meet the mandatory and preferred requirements in their response to this RFQ (Attachment 4). The resource(s) must meet the mandatory minimum requirements in order to be eligible for consideration as identified and set forth in Section 2.3.

Experience, including environments, must be fully documented.

The resource is required to have good oral and written skills. Additionally, the resource must have good organizational skills, proven analytical, planning, problem solving, and decision-making skills. It is required that the resource is knowledgeable in the English language and speak clearly and understandably using the English language.

During the interview process with the ODPS staff, the resource consultant(s) must demonstrate competence/experience in their specific area(s) of project assignment. The resource's experience must also be documented for review and verification. Offered resources not showing technical or functional competency/experience will be reason to reject the Offeror's quotation. It is the responsibility of the Offeror to pre-screen their candidates to ensure compliance.

Each RFQ response must include a profile for each resource consultant offered for the proposed ODPS Project.

4.5.9.1 References: Provide at least three (3) references for which each proposed resource has successfully demonstrated meeting the requirements of the Scope of Work on a project of similar size and scope in the previous five (5) years. The name of the person

to be contacted, phone number, company, address, brief description of project size and complexity, and dates (month and year) of employment must be given for each reference. Each resource must provide a list of professional references that can attest to his/her specific qualifications. The references given should be a person the candidate reported to and not a co-worker.

If less than three (3) references are provided, the Offeror must include information as to why less than three (3) references were provided. The State may disqualify the quotation if less than three (3) references are given (Attachment 2).

- 4.5.9.2 Education and Training: This section must be completed to list the education and training for each proposed candidate and will demonstrate, in detail, the proposed candidate's ability to properly execute the contract based on the relevance of the education and training to the requirements of the SOW (Attachment 3).
- 4.5.9.3 Resume: Each resource's resume must follow/support the above criteria and show how the resource meets the qualifications listed for the position in the SOW.
- 4.5.9.4 Mandatory Experience and Qualifications: The Offeror must complete this section to show how a resource meets the mandatory experience requirements, if any are applicable to that resource. If any resource does not meet the mandatory requirements for the position the resource is proposed to fill, the Offeror's Quotation may be rejected as non-responsive (Attachment 4).
- 4.5.9.5 Required Experience and Qualifications. The Offeror must complete this section, if applicable, to show how its resource meets the experience requirements (Attachment 4).

For each form submitted, the Offeror must provide the following information:

Instructor / Candidate's Name.

Contact Information. The Offeror must provide a client contact name, title, phone number, email address, company name, and mailing address. The Offeror also must include the same information for an alternate client contact, in case the State cannot reach the primary contact. Failure to provide this information or providing information that is inaccurate or out of date may result in the State not including the reference in the evaluation process or rejecting the Offeror's Quotation. The contact information given must be for a person within the client's organization and not a co-worker or a contact within the Offeror's organization, subsidiaries, partnerships, etc.

Dates of Experience. The Offeror must complete this section with a beginning month and year and an ending month and year to show the length of time the candidate performed the technical experience being described, not just the length of time the candidate worked for the company.

Description of the Related Service Provided. The State does not assume that, since the technical requirement is provided at the top of the page, all descriptions on that page relate to that requirement. Offerors must reiterate the technical experience being described, including the capacity in which the experience was performed and the role of the candidate in the work as it relates to the Work covered by this RFQ. It is the Offeror's responsibility to customize the description to clearly substantiate the candidate's qualification.

The candidate's work experience must be listed separately and completely every time it is referenced, regardless of whether it is on the same or different pages of the form.

4.5.10 Resource(s) Interview/Time Commitment:

The Offeror must agree to submit referenced resource(s) for interviews, in person at the ODPS discretion, during the period July 7, 2010 thru July 16, 2010 **No telephone interviews will be permitted. All interviews must be in person at the Ohio Department of Public Safety, Shipley Building, 1970 West Broad Street, Columbus, Ohio 43223.**

The Offeror must submit a statement and chart that clearly indicate the time commitment of each proposed resource to this assignment. The evaluation team may reject any quotation that commits any proposed resource to other projects/assignments during the term of the ODPS Project if the team believes that doing so will be detrimental to the Offeror's performance.

During the interview process the resource(s) must demonstrate their competency in their specific area(s) of project assignment. Additionally, the resource(s) must demonstrate excellent oral and written communication skills, knowledge in the English language, and their ability to speak clearly and understandably using the English language.

4.5.11 Offeror's Profile/Experience:

Each quotation must include a profile of the Offeror's relevant experience working on projects similar to this Project. The profile must also include the Offeror's legal name, address, and telephone number; home office location; date established; ownership (such as public firm, partnership, or subsidiary); firm leadership (such as corporate officers or partners); number of years in business, number of employees; number of employees engaged in work directly related to the Project; corporate information which demonstrates the depth of the company and the Offeror's ability to provide support and backup for proposed personnel and any other background information that will help the evaluation team gauge the ability of the Offeror to successfully complete the Project (Attachments 5 and 6).

4.5.12 Offeror References:

The Offeror must include at least three (3) references for which the Offeror has successfully provided services on projects that were similar in their nature, size, and scope to this Project. These references must be from projects that were completed within the previous five (5) years.

The State is interested in the Offeror's performance and responsibility in projects such as Public Safety's. References provided must agree to be interviewed by the State concerning the Offeror's products and services. Failure to provide three references may result in disqualification of quotation.

The following information is required for each reference:

4.5.12.1 Customer's name and address.

4.5.12.2 Contact name, title, and current phone number.

4.5.12.3 Date contract began and date completed.

4.5.12.4 Summary of the scope of the project and an explanation as to the relevance or similarity to this project and the type of reference being requested (Attachment 7).

4.5.13 Contract Performance:

The Offeror must provide the contract performance information for the past seven (7) years (Attachment 8).

4.5.14 A Contract between the Ohio Department of Public Safety and the Contractor:

The Offeror must submit a completed and signed contract signature page (Attachment 9).

5 Evaluation

5.1 **Review of Quotations:**

An evaluation team has been formed to determine the responsiveness of the quotations. The team shall be comprised of the ODPS personnel.

5.2 **Rejection of any/all quotations:**

5.2.1 The ODPS may reject any quotations, in whole or in part, and may determine that any irregularities or deviations from the specifications do not result in determining the quotation is non-responsive.

The Chief of Purchasing may wave irregularities or deviations only if doing so does not affect the amount of the quotation or result in an unfair competitive advantage to any Offeror.

5.2.2 The ODPS reserves the right to disqualify an Offeror's response and any quotations for the following reasons:

5.2.2.1 Failure to provide a signed original quotation (signature in Blue Ink).

5.2.2.2 Late RFQ responses.

5.2.2.3 Failure to provide required information and/or meet specifications.

5.2.2.4 Failure to offer services completely covered by a current STS contract with the state of Ohio.

5.2.3 In addition, should the quotations exceed the planned budget for this service; the ODPS may reject the quotations or try to negotiate a lower price.

5.3 Evaluation Criteria:

Factors that will determine the most responsive quotation shall be the costs and the evaluation factors listed below in order of importance. Factors include, but, are not limited to, the following:

5.3.1 Offerors proposed team's experience and skills.

5.3.2 Offeror profile.

5.3.3 Offeror references demonstrating the ability to complete this project based upon similar previous experience.

5.3.4 Offeror's expected ODPS personnel staffing commitment to complete this Project within the expected timeframe.

5.4 Basis of Award:

The award will be made to the lowest, responsive and responsible Offeror meeting the qualifications specified in this RFQ.

Balance of this page was intentionally left blank

ATTACHMENT 1**QUOTATION/COST SUMMARY TABLE**

Offerors will complete the Quotation/Cost Summary table, below, and identify all costs associated with performing the work. The ODPS is expecting that the rates quoted shall be significantly discounted from the STS rates.

The Offeror shall include the Proposed Instructor, STS Schedule Part / Item Number and STS Title / Description, STS rate, discount rate (percentage off STS list price), Offered Costs per course per participant, and the Extended Cost (Offered Cost times Quantity) in response to this Scope of Work. If needed, the Offeror may include additional costs as determined by the Offeror to complete the RFQ. The following table must be completed with this information.

(The following tables assume that the vendor will be selected by July 16, 2010, will begin work in September, 2010 and complete the work by June 30, 2011).

Offeror Name: _____

OHIO STS-033 **Schedule Number:** _____ **Current Expiration Date:** _____

Description of Training	Proposed Instructor	STS Vendor Part / Item Number (See Note 1)	STS Title / Description (See Note 1)	STS Rate	Disc. Rate	Offered Cost	Quantity (See Note 2)	Total Cost
CompTIA A+ Training				\$	\$	\$	20	\$
CompTIA Network+				\$	\$	\$	20	\$
Total Not-to-Exceed Fixed Cost								\$

Cost for a Participant to take the optional CompTIA A+ Essentials examination (Not paid by the State) *	\$
Cost for a Participant to take the optional CompTIA Practical Application examination (Not paid by the State) *	\$
Cost for a Participant to take the optional CompTIA Network+ examination (Not paid by the State) *	\$

Note 1: STS Vendor Part / Item Number and STS Title / Description must match categories listed and approved on the current Ohio STS identified above.

Note 2: The ODPSS reserves the right to add participants to the training sessions at the offered rate.

* **Will not be used in the evaluation.**

ATTACHMENT 2
INSTRUCTOR REFERENCES

Candidate's Name:

Three (3) professional references who have received services from the candidate in the past five (5) years.

Company Name:	Contact Name:	
Address:	Phone Number:	
Project Name:	Beginning Date of Project Month/Year:	Ending Date of Project Month/Year:
Description of project size, complexity and the candidate's role in this project.		

Company Name:	Contact Name:	
Address:	Phone Number:	
Project Name:	Beginning Date of Project Month/Year:	Ending Date of Project Month/Year:
Description of project size, complexity and the candidate's role in this project.		

Company Name:	Contact Name:	
Address:	Phone Number:	
Project Name:	Beginning Date of Project Month/Year:	Ending Date of Project Month/Year:
Description of project size, complexity and the candidate's role in this project.		

Note: A routine background check will be processed by the Ohio Department of Public Safety as soon as possible after the candidate has been accepted. Failure to pass the background check may result in immediate dismissal of the candidate; whereupon, the Offeror must submit a replacement candidate within the time limits as set forth in 3.7 Replacement Personnel of this RFQ.

**ATTACHMENT 3
INSTRUCTOR EDUCATION AND TRAINING**

Candidate's Name:

This section must be completed to list the education and training of the proposed candidate(s).

Education and Training	Months/Years	Where Obtained	Degree/Major Year Earned
College			
Technical School			
Other Training			

ATTACHMENT 4

INSTRUCTOR EXPERIENCE REQUIREMENT

Candidate's Name:

MANDATORY REQUIREMENT 2.3.1: Five (5) years of technical instruction experience, with a minimum of three (3) years in CompTIA A+ and Network+ certification preparation.

Client's Company Name:	Client's Project Supervisor Contact Name:	
Address:	Phone Number:	
Project Name:	Beginning Date of Project Month/Year:	Ending Date of Project Month/Year:
Description of the related services provided:		

Client's Company Name:	Client's Project Supervisor Contact Name:	
Address:	Phone Number:	
Project Name:	Beginning Date of Project Month/Year:	Ending Date of Project Month/Year:
Description of the related services provided:		

Client's Company Name:	Client's Project Supervisor Contact Name:	
Address:	Phone Number:	
Project Name:	Beginning Date of Project Month/Year:	Ending Date of Project Month/Year:
Description of the related service provided:		

ATTACHMENT 4

CANDIDATE(S) EXPERIENCE REQUIREMENT

Candidate's Name:

MANDATORY REQUIREMENT 2.3.2: Five (5) years of hands-on work experience involving tasks (See Supplement One, Two, and Three) associated with the objectives identified by CompTIA as required knowledge for the A+ and Network+ certification examinations.

Client's Company Name:	Client's Project Supervisor Contact Name:	
Address:	Phone Number:	
Project Name:	Beginning Date of Project Month/Year:	Ending Date of Project Month/Year:
Description of the related services provided:		

Client's Company Name:	Client's Project Supervisor Contact Name:	
Address:	Phone Number:	
Project Name:	Beginning Date of Project Month/Year:	Ending Date of Project Month/Year:
Description of the related services provided:		

Client's Company Name:	Client's Project Supervisor Contact Name:	
Address:	Phone Number:	
Project Name:	Beginning Date of Project Month/Year:	Ending Date of Project Month/Year:
Description of the related service provided:		

**ATTACHMENT 6
OFFEROR EXPERIENCE FORM**

The Offeror must provide examples of experience:

Mandatory Offeror Requirement 2.2.1: The Offeror must have the appropriate facilities, located within Franklin County, Ohio and the equipment to facilitate training of participants and allow participants to take the CompTIA certification exams onsite, immediately following the completion of each course.		
Customer No. 1:	City & State:	
Contact:	Telephone:	
Title:	From:	To:
Customer No. 2:	City & State:	
Contact:	Telephone:	
Title:	From:	To:
Customer No. 3:	City & State:	
Contact:	Telephone:	
Title:	From:	To:

ATTACHMENT 7

OFFEROR CUSTOMER REFERENCE FORM

Reference No. One		
Company Name:		Telephone:
Contact Name:		Extension:
City, State, & Zip:		
Program Name:		
Dates of Service:		
Description of Related Service Provided:		

Reference No. Two		
Company Name:		Telephone:
Contact Name:		Extension:
City, State, & Zip:		
Program Name:		
Dates of Service:		
Description of Related Service Provided:		

Reference No. Three		
Company Name:		Telephone:
Contact Name:		Extension:
City, State, & Zip:		
Program Name:		
Dates of Service:		
Description of Related Service Provided:		

ATTACHMENT 8**CONTRACT PERFORMANCE**

The Offeror must provide the following information for this section for the past seven years. Please indicate yes or no in each row.

Yes/No	Description
	Whether the Offeror has had a contract terminated for default or cause. If so, the Offeror must submit full details, including the other party's name, address, and telephone number.
	Whether the Offeror has been assessed any penalties in excess of five thousand dollars (\$5,000), including liquidated damages, under any of its existing or past contracts with any organization (including any government entity). If so, the Offeror must provide complete details, including the name of the other organization, the reason for the penalty, and the penalty amount for each incident.
	Whether the Offeror was the subject of any governmental action limiting the right of the Offeror to do business with that entity or any other governmental entity.
	Whether trading in the stock of the company has ever been suspended with the date(s) and explanation(s).
	Whether the Offeror, any officer of the Offeror, or any owner of a 20% interest or greater in the Offeror has filed for bankruptcy, reorganization, a debt arrangement, moratorium, or any proceeding under any bankruptcy or insolvency law, or any dissolution or liquidation proceeding.
	Whether the Offeror, any officer of the Offeror, or any owner with a 20% interest or greater in the Offeror has been convicted of a felony or is currently under indictment on any felony charge.

If the answer to any item is affirmative, the Offeror must provide complete details about the matter. While an affirmative answer to any of these items will not automatically disqualify an Offeror from consideration, at the sole discretion of the evaluation team, such an answer and a review of the background details may result in a rejection of the Offeror's quotation. The team will make this decision based on its determination of the seriousness of the matter, the matter's possible impact on the Offeror's performance on the project, and the best interests of the State.

ATTACHMENT 9

A CONTRACT BETWEEN
THE OHIO DEPARTMENT OF PUBLIC SAFETY
AND

(CONTRACTOR)

THIS CONTRACT, which results from **RFQ 11-162, Technical Training for Mainframe Resources**, is between the state of Ohio, Department of Public Safety (the "State"), and _____ (the "Contractor").

If this RFQ results in a contract award, the Contract will consist of this RFQ including all attachments, written amendments to this RFQ, the Contractor's quotation, and written, authorized amendments to the Contractor's quotation. It will also include any materials incorporated by reference in the above documents and any purchase orders and change orders issued under the Contract. The form of the Contract is this one page attachment to the RFQ, which incorporates by reference all the documents identified above. The terms and conditions for the Contract are contained in this RFQ. If there are conflicting provisions between the documents that make up the contract, the order of preference for the documents is as follows:

1. This Project and Contract is governed by State Term Schedule No. _____. If there are any conflicts between the State Term Schedule and this Contract, the State Term Schedule will prevail;
2. This RFQ, as amended;
3. The documents and materials incorporated by reference in the RFQ;
4. The Contractor's quotation, as amended, clarified, and accepted by the State; and
5. The documents and materials incorporated by reference in the Contractor's quotation.

Notwithstanding the order listed above, purchase orders, change orders, and amendments issued after the contract is executed may expressly change the provisions of the contract. If they do so expressly, then the most recent of them will take precedence over anything else that is part of the contract.

This contract has an effective date of the later of _____, 2010, or the occurrence of all conditions precedent specified in the Terms and Conditions.

IN WITNESS WHEREOF, the parties have executed this Contract as of the dates below.

CONTRACTOR

STATE OF OHIO
DEPARTMENT OF PUBLIC SAFETY

By:

By: Thomas J. Stickrath, Director

Title:

Ohio Department of Public Safety

Date:

Date:

ATTACHMENT 10

**Background Information Form
(Non-ODPS Employee)**



**FACILITY ACCESS CARD REQUEST
NON-ODPS EMPLOYEE**

ODPS SPONSOR INFORMATION (ODPS employee responsible for individual requiring access)

OHIO DEPARTMENT OF PUBLIC SAFETY SPONSOR NAME	
SPONSOR DIV/SECTION/UNIT	SPONSOR PHONE # () -
SPONSOR SIGNATURE X	
REQUEST ACCESS BE GRANTED TO (building/location)	
TYPE OF ACCESS:	START DATE / /
<input type="checkbox"/> PICTURE ACCESS CARD WITH ACCESS RIGHTS	END DATE / /
<input type="checkbox"/> SIGN IN AND SIGN OUT/VISITORS BADGE	
REASON FOR ACCESS	

COMPANY OR AGENCY INFORMATION

COMPANY NAME		
ADDRESS		
CITY	STATE	ZIP CODE
EMERGENCY OFFICE PHONE # () -		
COMPANY SIGNATURE (i.e., Corporate Officer, Chief) X	PRINT NAME	

INFORMATION ON INDIVIDUAL REQUIRING ACCESS

LAST NAME	FIRST NAME	FULL MIDDLE NAME	
PRESENT ADDRESS	CITY	STATE	ZIP CODE
DATE OF BIRTH: (MM/DD/YY) / /	AUTO-GENERATED PIN #		
ALIASES AND/OR MAIDEN NAME	HOME PHONE # () -		
YOUR SUPERVISOR'S NAME (print)	SUPERVISOR OFFICE PHONE # () -		
LIST ANY FELONY OR MISDEMEANOR CONVICTIONS IN THE PAST TEN YEARS AND DATE OF CONVICTION:			
DRIVER LICENSE #/STATE ID/PASSPORT (ATTACH COPY OF LEGAL PICTURE ID)			
I _____, CERTIFY THAT ALL OF THE ANSWERS AND STATEMENTS ON THIS FORM ARE COMPLETE, TRUE, AND CORRECT TO THE BEST OF MY KNOWLEDGE AND ARE MADE IN GOOD FAITH.			
SIGNATURE X			DATE

SUBMIT TO YOUR SPONSOR 30 DAYS PRIOR TO ARRIVING AT THE SITE. SPONSOR WILL COORDINATE THE ISSUANCE OF AN ODPS ACCESS CARD.

(DPS-505.02)

DPS 0166 4/10

ATTACHMENT 11

NONDISCLOSURE AGREEMENT

This Nondisclosure Agreement (“**Agreement**”) is made this ____ day of _____, 20____
by _____ (“**Contractor**”)

WHEREAS, Contractor holds a position of trust relative to the information received during the performance of the work on the project. By executing this Agreement, Contractor acknowledges and recognizes the responsibility entrusted to Contractor and to the state of Ohio in preserving the security and confidentiality of the information.

NOW THEREFORE, Contractor agrees as follows:

- 1.** The term "**Confidential Information**" shall mean any and all information which is disclosed by the State verbally, electronically, visually, or in a written or other tangible form that is not generally disclosed to the public, including but not limited to, trade secrets, computer programs, software, software manuals and documentation, technology, systems, source code, databases, applications, engine protocols, routines, models, displays and manuals, including, without limitation, the selection, coordination and arrangement of the contents thereof, formulas, data, inventions, methodologies, algorithms, techniques, processes, research activities and plans, marketing and sales plans, strategic plans, forecasts, training materials, pricing and pricing strategies, methods of operation, internal controls, security procedures, third party confidential information, customer lists, unpublished financial information, and personal information such as social security numbers, home addresses, telephone numbers, emergency contact information, and any other personal information.
- 2.** Contractor warrants and agrees to keep Confidential Information in strict confidence and shall not disclose it to any third party. Contractor shall use Confidential Information in a manner consistent with the terms of this Agreement and only in furtherance of the work on the project. Contractor's internal disclosure of Confidential Information shall be only to those employees, contractors or agents having a need to know such information in connection with this Agreement and only insofar as such persons are bound by a nondisclosure agreement consistent with this Agreement. Contractor shall promptly notify the State of any unauthorized disclosure or use of Confidential Information by any person and/or entity. Upon termination of this Agreement, or the State's written request, the Contractor shall cease use of the Confidential Information and immediately return all tangible Confidential Information to the State. With respect to Confidential Information stored in electronic form, the Contractor shall delete all such Confidential Information from its systems and certify in writing to the State that such information has been deleted.
- 3.** This Agreement imposes no obligation upon Contractor with respect to Confidential Information which Contractor can establish by legally sufficient evidence that such information: (a) was, prior to receipt from the State, in the possession of, or was rightfully known by Contractor, without an obligation to maintain its confidentiality; (b) is or becomes generally known to the public without violation of this Agreement or without a violation of an obligation of confidentiality owed to the State; (c) is obtained by Contractor in good faith from a third party having the right to disclose it without an obligation of confidentiality; or (d) is independently developed by Contractor without the use of or reference to the Confidential Information. Contractor may disclose Confidential Information in accordance with valid judicial or other governmental order, provided that Contractor shall have given the State reasonable notice and opportunity to object prior to such disclosure, will seek confidential treatment of the information disclosed, and shall comply with any applicable protective order or equivalent.
- 4.** The Confidential Information is provided “as-is” and the State makes no representation or warranty of any kind, express or implied, with respect to the suitability, accuracy or non-infringement of third party rights. The

State shall at all times retain sole and exclusive title to, ownership of, all rights in and control over the use of all its Confidential Information. Contractor agrees that nothing in this Agreement is intended to grant any rights or license under any intellectual property rights of the State, nor shall this Agreement grant Contractor any rights in or to the Confidential Information, except the limited right to use such information in accordance with this Agreement.

5. Contractor will be liable for the disclosure of Confidential Information whether the disclosure is intentional, negligent, or accidental, and that breach of this Agreement may result in Contractor and Contractor's organization being prohibited from participating in any future work with the Ohio Department of Public Safety.

6. This Agreement constitutes the entire agreement and supersedes all prior understandings and agreements concerning this subject matter. All additions or modifications to this Agreement must be in writing and signed by the authorized representatives of both parties. This Agreement shall be governed by the laws of the state of Ohio, excluding choice of law principles. Contractor acknowledges that monetary damages may not be sufficient remedy for unauthorized use or disclosure of Confidential Information, or for breach of this Agreement, and the State shall be entitled, without waiving any other rights or remedies, to such injunctive or equitable relief as may be deemed proper by a court of competent jurisdiction.

Contractor has read and understands this Nondisclosure Agreement. Contractor's signature below indicates Contractor's agreement to all of the above terms.

BY: _____

TITLE: _____

SIGNATURE: _____

DATE: _____

ATTACHMENT 12

CONFIDENTIALITY AND CONDUCT AGREEMENT

As part of this engagement by you with the state of Ohio, you hold a position of trust relative to the information received during the performance of the Work. By executing this Confidentiality and Conduct Agreement, you acknowledge and recognize the responsibility entrusted to you and to the state of Ohio in preserving the security and confidentiality of the information.

I will not disclose any confidential and/or sensitive information to third parties, unless otherwise authorized in writing by the State to do so.

I will use any confidential or sensitive information solely to do the Work.

I will restrict circulation of confidential and/or sensitive information within my organization and then only to people in my organization that have a need to know to do the Work.

Title to confidential and/or sensitive information and all related materials and documentation the State delivers to me will remain with the State.

I will be liable for the disclosure of such information whether the disclosure is intentional, negligent, or accidental.

I will not incorporate any portion of any confidential and/or sensitive information into anything, other than a Deliverable, and will have no proprietary interest in any of the confidential and/or sensitive information.

I will return all originals of any confidential information and destroy any copies I have made on termination or expiration of this project.

I will destroy any sensitive information (notes, work documents, documentation, etc.) that I have accumulated while doing the Work upon termination or expiration of this project.

I understand that I am not a representative of the state of Ohio and will not represent myself as such unless requested in writing by the State.

I understand that breach of this Agreement may result in my organization and I being prohibited from participating in any future work related to this project.

I have read and understand the Confidentiality and Conduct Agreement. My signature below indicates my agreement to all of the above terms.

BY: _____
(PLEASE PRINT)

TITLE: _____

SIGNATURE : _____

DATE: _____

SUPPLEMENT ONE

CompTIA A+ Essentials (2009 Edition) Objectives Exam Number: 220-701

Introduction

In order to receive CompTIA A+ certification a candidate must pass two exams. The first exam is CompTIA A+ Essentials, exam number 220-701. The CompTIA A+ Essentials examination measures necessary competencies for an entry-level IT professional with the equivalent knowledge of at least 500 hours of hands-on experience in the lab or field. Successful candidates will have the knowledge required to understand the fundamentals of computer technology, networking, and security, and will have the skills required to identify hardware, peripheral, networking, and security components. Successful candidates will understand the basic functionality of the operating system and basic troubleshooting methodology, practice proper safety procedures, and will effectively interact with customers and peers.

CompTIA A+ is ISO 17024 Accredited (Personnel Certification Accreditation) and, as such, undergoes regular reviews and updates to the exam objectives. The following CompTIA A+ Essentials objectives reflect the subject areas in the 2009 Edition of the exam and result from subject matter expert workshops and industry-wide survey results regarding the skills and knowledge required of an entry-level IT professional. The percentages in this document represent the relative importance of the subject areas (domains) in the associated body of knowledge, and together establish the foundation of an entry-level IT professional.

This examination blueprint includes domain weighting, test objectives, and example content. Example topics and concepts are included to clarify the test objectives and should not be construed as a comprehensive listing of all the content of this examination.

Candidates are encouraged to use this document to guide their studies. The contents of the examination blueprint help prioritize topics and provide a guide of what to expect on the CompTIA A+ Essentials exam. The table below lists the domains measured by this examination and the extent to which they are represented. The CompTIA A+ Essentials (2009 Edition) exam is based on these objectives.

Domain	Percentage of Examination
1.0 Hardware	27%
2.0 Troubleshooting, Repair & Maintenance	20%
3.0 Operating System and Software	20%
4.0 Networking	15%
5.0 Security	8%
6.0 Operational Procedure	10%
Total	100%

****Note:** The lists of examples provided in bulleted format below each objective are not exhaustive lists. Other examples of technologies, processes or tasks pertaining to each objective may also be included on the exam though not listed or covered in this objectives document.

CompTIA is constantly reviewing the content of our exams and updating test questions to be sure our exams are current and the security of the questions is protected. When necessary, we will publish updated exams based on existing exam objectives. Please know that all related exam preparation materials will still be valid.

1.0 Hardware

1.1 Categorize storage devices and backup media

- FDD
 - HDD
 - Solid state vs. magnetic
 - Optical drives
 - CD / DVD / RW / Blu-Ray
 - Removable storage
 - Tape drive
 - Solid state (e.g. thumb drive, flash, SD cards, USB)
 - External CD-RW and hard drive
 - Hot swappable devices and non-hot swappable devices

1.2 Explain motherboard components, types and features

- Form Factor
 - ATX / BTX,
 - micro ATX
 - NLX
- I/O interfaces
 - Sound
 - Video
 - USB 1.1 and 2.0
 - Serial
 - IEEE 1394 / Firewire
 - Parallel
 - NIC
 - Modem
 - PS/2
- Memory slots
 - RIMM
 - DIMM
 - SODIMM
 - SIMM
- Processor sockets
- Bus architecture
- Bus slots
 - PCI
 - AGP
 - PCIe
 - AMR
 - CNR
 - PCMCIA
- PATA
 - IDE
 - EIDE
- SATA, eSATA
- Contrast RAID (levels 0, 1, 5)
- Chipsets
- BIOS / CMOS / Firmware
 - POST
 - CMOS battery
- Riser card / daughterboard

1.3 Classify power supplies types and characteristics

- AC adapter
- ATX proprietary
- Voltage, wattage and capacity
- Voltage selector switch
- Pins (20, 24)

- 1.4 Explain the purpose and characteristics of CPUs and their features**
- . Identify CPU types
 - AMD
 - Intel
 - . Hyper threading
 - . Multi core
 - Dual core
 - Triple core
 - Quad core
 - . Onchip cache
 - L1
 - L2
 - . Speed (real vs. actual)
 - . 32bit vs. 64 bit
- 1.5 Explain cooling methods and devices**
- . Heat sinks
 - . CPU and case fans
 - . Liquid cooling systems
 - . Thermal compound
- 1.6 Compare and contrast memory types, characteristics and their purpose**
- . Types
 - DRAM
 - SRAM
 - SDRAM
 - DDR / DDR2 / DDR3
 - RAMBUS
 - . Parity vs. Non-parity
 - . ECC vs. non-ECC
 - . Single sided vs. double sided
 - . Single channel vs. dual channel
 - . Speed
 - PC100
 - PC133
 - PC2700
 - PC3200
 - DDR3-1600
 - DDR2-667
- 1.7 Distinguish between the different display devices and their characteristics**
- . Projectors, CRT and LCD
 - . LCD technologies
 - Resolution (e.g. XGA, SXGA+, UXGA, WUXGA)
 - Contrast ratio
 - Native resolution
 - . Connector types
 - VGA
 - HDMi
 - S-Video
 - Component / RGB
 - DVI pin compatibility
 - . Settings
 - Refresh rate
 - Resolution
 - Multi-monitor
 - Degauss

1.8 Install and configure peripherals and input devices

- . Mouse
- . Keyboard
- . Bar code reader
- . Multimedia (e.g. web and digital cameras, MIDI, microphones)
- . Biometric devices
- . Touch screen
- . KVM switch

1.9 Summarize the function and types of adapter cards

- . Video
 - PCI
 - PCIe
 - AGP
- . Multimedia
 - Sound card
 - TV tuner cards
 - Capture cards
- . I/O
 - SCSI
 - Serial
 - USB
 - Parallel
- . Communications
 - NIC
 - Modem

1.10 Install, configure and optimize laptop components and features

- . Expansion devices
 - PCMCIA cards
 - PCI Express cards
 - Docking station
- . Communication connections
 - Bluetooth
 - Infrared
 - Cellular WAN
 - Ethernet
 - Modem
- . Power and electrical input devices
 - Auto-switching
 - Fixed input power supplies
 - Batteries
- . Input devices
 - Stylus / digitizer
 - Function keys
 - Point devices (e.g. touch pad, point stick / track point)

1.11 Install and configure printers

- . Differentiate between printer types
 - Laser
 - Inkjet
 - Thermal
 - Impact
- . Local vs. network printers
- . Printer drivers (compatibility)
- . Consumables

2.0 Troubleshooting, Repair and Maintenance

2.1 Given a scenario, explain the troubleshooting theory

- Identify the problem
 - Question the user and identify user changes to computer and perform backups before making changes
- Establish a theory of probable cause (question the obvious)
- Test the theory to determine cause
 - Once theory is confirmed determine next steps to resolve problem
 - If theory is not confirmed re-establish new theory or escalate
- Establish a plan of action to resolve the problem and implement the solution
- Verify full system functionality and if applicable implement preventative measures
- Document findings, actions and outcomes

2.2 Given a scenario, explain and interpret common hardware and operating system symptoms and their causes

- OS related symptoms
 - Bluescreen
 - System lock-up
 - Input/output device
 - Application install
 - Start or load
 - Windows specific printing problems
 - Print spool stalled
 - Incorrect / incompatible driver
- Hardware related symptoms
 - Excessive heat
 - Noise
 - Odors
 - Status light indicators
 - Alerts
 - Visible damage (e.g. cable, plastic)
- Use documentation and resources
 - User / installation manuals
 - Internet / web based
 - Training materials

2.3 Given a scenario, determine the troubleshooting methods and tools for printers

- Manage print jobs
- Print spooler
- Printer properties and settings
- Print a test page

2.4 Given a scenario, explain and interpret common laptop issues and determine the appropriate basic troubleshooting method

- Issues
 - Power conditions
 - Video
 - Keyboard
 - Pointer
 - Stylus
 - Wireless card issues
- Methods
 - Verify power (e.g. LEDs, swap AC adapter)
 - Remove unneeded peripherals
 - Plug in external monitor
 - Toggle Fn keys or hardware switches
 - Check LCD cutoff switch
 - Verify backlight functionality and pixilation
 - Check switch for built-in WIFI antennas or external antennas

2.5 Given a scenario, integrate common preventative maintenance techniques

- . Physical inspection
- . Updates
 - Driver
 - Firmware
 - OS
 - Security
- . Scheduling preventative maintenance
 - Defrag
 - Scandisk
 - Check disk
 - Startup programs
- . Use of appropriate repair tools and cleaning materials
 - Compressed air
 - Lint free cloth
 - Computer vacuum and compressors
- . Power devices
 - Appropriate source such as power strip, surge protector or UPS
- . Ensuring proper environment
- . Backup procedures

3.0 Operating Systems and Software - Unless otherwise noted, operating systems referred to within include Microsoft Windows 2000, Windows XP Professional, XP Home, XP MediaCenter, Windows Vista Home, Home Premium, Business and Ultimate.

3.1 Compare and contrast the different Windows Operating Systems and their features

- . Windows 2000, Windows XP 32bit vs. 64bit, Windows Vista 32 bit vs. 64bit
 - Side bar, Aero, UAC, minimum system requirements, system limits
 - Windows 2000 and newer – upgrade paths and requirements
 - Terminology (32bit vs. 64bit – x86 vs. x64)
 - Application compatibility, installed program locations (32bit vs. 64bit), Windows compatibility mode
 - User interface, start bar layout

3.2 Given a scenario, demonstrate proper use of user interfaces

- . Windows Explorer
- . My Computer
- . Control Panel
- . Command prompt utilities
 - telnet
 - ping
 - ipconfig
- . Run line utilities
 - msconfig
 - msinfo32
 - DxDiag
 - Cmd
 - REGEDIT
- . My Network Places
- . Task bar / systray
- . Administrative tools
 - Performance monitor, Event Viewer, Services, Computer Management
 - MMC
- . Task Manager
- . Start Menu

3.3 Explain the process and steps to install and configure the Windows OS

- . File systems
 - FAT32 vs. NTFS
- . Directory structures
 - Create folders
 - Navigate directory structures
- . Files
 - Creation
 - Extensions
 - Attributes
 - Permissions
- . Verification of hardware compatibility and minimum requirements
- . Installation methods
 - Boot media such as CD, floppy or USB
 - Network installation
 - Install from image
 - Recover CD
 - Factory recovery partition
- . Operating system installation options
 - File system type
 - Network configuration
 - Repair install
- . Disk preparation order
 - Format drive
 - Partition
 - Start installation

- . Device Manager
 - Verify
 - Install and update devices drivers
 - Driver signing
- . User data migration – User State Migration Tool (USMT)
- . Virtual memory
- . Configure power management
 - Suspend
 - Wake on LAN
 - Sleep timers
 - Hibernate
 - Standby
- . Demonstrate safe removal of peripherals

3.4 Explain the basics of boot sequences, methods and startup utilities

- . Disk boot order / device priority
 - Types of boot devices (disk, network, USB, other)
- . Boot options
 - Safe mode
 - Boot to restore point
 - Recovery options
 - Automated System Recovery (ASR)
 - Emergency Repair Disk (ERD)
 - Recovery console

4.0 Networking

4.1 Summarize the basics of networking fundamentals, including technologies, devices and protocols

- . Basics of configuring IP addressing and TCP/IP properties (DHCP, DNS)
- . Bandwidth and latency
- . Status indicators
- . Protocols (TCP/IP, NETBIOS)
- . Full-duplex, half-duplex
- . Basics of workgroups and domains
- . Common ports: HTTP, FTP, POP, SMTP, TELNET, HTTPS
- . LAN / WAN
- . Hub, switch and router
- . Identify Virtual Private Networks (VPN)
- . Basics class identification

4.2 Categorize network cables and connectors and their implementations

- . Cables
 - Plenum / PVC
 - UTP (e.g. CAT3, CAT5 / 5e, CAT6)
 - STP
 - Fiber
 - Coaxial cable
- . Connectors
 - RJ45
 - RJ11

4.3 Compare and contrast the different network types

- . Broadband
 - DSL
 - Cable
 - Satellite
 - Fiber
- . Dial-up
- . Wireless
 - All 802.11 types
 - WEP
 - WPA
 - SSID
 - MAC filtering
 - DHCP settings
- . Bluetooth
- . Cellular

5.0 Security

5.1 Explain the basic principles of security concepts and technologies

- . Encryption technologies
- . Data wiping / hard drive destruction / hard drive recycling
- . Software firewall
 - Port security
 - Exceptions
- . Authentication technologies
 - User name
 - Password
 - Biometrics
 - Smart cards
- . Basics of data sensitivity and data security
 - Compliance
 - Classifications
 - Social engineering

5.2 Summarize the following security features

- . Wireless encryption
 - WEPx and WPAX
 - Client configuration (SSID)
- . Malicious software protection
 - Viruses
 - Trojans
 - Worms
 - Spam
 - Spyware
 - Adware
 - Grayware
- . BIOS Security
 - Drive lock
 - Passwords
 - Intrusion detection
 - TPM
- . Password management / password complexity
- . Locking workstation
 - Hardware
 - Operating system
- . Biometrics
 - Fingerprint scanner

6.0 Operational Procedure

6.1 Outline the purpose of appropriate safety and environmental procedures and given a scenario apply them

- . ESD
- . EMI
 - Network interference
 - Magnets
- . RFI
 - Cordless phone interference
 - Microwaves
- . Electrical safety
 - CRT
 - Power supply
 - Inverter
 - Laser printers
 - Matching power requirements of equipment with power distribution and UPSs
- . Material Safety Data Sheets (MSDS)
- . Cable management
 - Avoiding trip hazards
- . Physical safety
 - Heavy devices
 - Hot components
- . Environmental – consider proper disposal procedures

6.2 Given a scenario, demonstrate the appropriate use of communication skills and professionalism in the workplace

- . Use proper language – avoid jargon, acronyms, slang
- . Maintain a positive attitude
- . Listen and do not interrupt a customer
- . Be culturally sensitive
- . Be on time
 - If late contact the customer
- . Avoid distractions
 - Personal calls
 - Talking to co-workers while interacting with customers
 - Personal interruptions
- . Dealing with a difficult customer or situation
 - Avoid arguing with customers and/or being defensive
 - Do not minimize customers' problems
 - Avoid being judgmental
 - Clarify customer statements
 - Ask open-ended questions to narrow the scope of the problem
 - Restate the issue or question to verify understanding
- . Set and meet expectations / timeline and communicate status with the customer
 - Offer different repair / replacement options if applicable
 - Provide proper documentation on the services provided
 - Follow up with customer / user at a later date to verify satisfaction
- . Deal appropriately with customers confidential materials
 - Located on computer, desktop, printer, etc.

CompTIA A+ Acronyms

Introduction

The following is a list of acronyms which appear on the CompTIA A+ exams. Candidates are encouraged to review the complete list and attain a working knowledge of all listed acronyms as a part of a comprehensive exam preparation program.

ACRONYM SPELLED OUT

AC	alternating current
ACL	access control list
ACPI	advanced configuration and power interface
ACT	activity
ADSL	asymmetrical digital subscriber line
AGP	accelerated graphics port
AMD	advanced micro devices
APIPA	automatic private internet protocol addressing
APM	advanced power management
ARP	address resolution protocol
ASR	automated system recovery
AT	advanced technology
ATA	advanced technology attachment
ATAPI	advanced technology attachment packet interface
ATM	asynchronous transfer mode
ATX	advanced technology extended
BIOS	basic input/output system
BNC	Bayonet-Neill-Concelman or British Naval Connector
BTX	balanced technology extended
CD	compact disc
CD-ROM	compact disc-read-only memory
CD-RW	compact disc-rewritable
CDFS	compact disc file system
CFS	Central File System, Common File System, Command File System
CMOS	complementary metal-oxide semiconductor
COMx	communication port (x=port number)
CPU	central processing unit
CRT	cathode-ray tube
DAC	discretionary access control
DB-25	serial communications D-shell connector, 25 pins
DB-9	9 pin D shell connector
DC	direct current
DDOS	distributed denial of service
DDR	double data-rate
DDR RAM	double data-rate random access memory
DDR SDRAM	double data-rate synchronous dynamic random access memory
DFS	distributed file system
DHCP	dynamic host configuration protocol
DIMM	dual inline memory module
DIN	Deutsche Industrie Norm
DIP	dual inline package
DLT	digital linear tape
DLP	digital light processing
DMA	direct memory access
DMZ	demilitarized zone
DNS	domain name service or domain name server
DOS	denial of service
DPMS	display power management signaling
DRAM	dynamic random access memory
DSL	digital subscriber line
DVD	digital video disc or digital versatile disc
DVD-RAM	digital video disc-random access memory

DVD-ROM	digital video disc-read only memory
DVD-R	digital video disc-recordable
DVD-RW	digital video disc-rewritable
DVI	digital visual interface
ECC	error correction code
ECP	extended capabilities port
EEPROM	electrically erasable programmable read-only memory
EFS	encrypting file system
EIDE	enhanced integrated drive electronics
EMI	electromagnetic interference
EMP	electromagnetic pulse
EPROM	erasable programmable read-only memory
EPP	enhanced parallel port
ERD	emergency repair disk
ESD	electrostatic discharge
EVGA	extended video graphics adapter/array
EVDO	evolution data optimized or evolution data only
FAT	file allocation table
FAT12	12-bit file allocation table
FAT16	16-bit file allocation table
FAT32	32-bit file allocation table
FDD	floppy disk drive
Fn	Function (referring to the function key on a laptop)
FPM	fast page-mode
FRU	field replaceable unit
FSB	Front Side Bus
FTP	file transfer protocol
FQDN	fully qualified domain name
Gb	gigabit
GB	gigabyte
GDI	graphics device interface
GHz	gigahertz
GUI	graphical user interface
GPS	global positioning system
GSM	global system for mobile communications
HAL	hardware abstraction layer
HCL	hardware compatibility list
HDD	hard disk drive
HDMI	high definition media interface
HPFS	high performance file system
HTML	hypertext markup language
HTTP	hypertext transfer protocol
HTTPS	hypertext transfer protocol over secure sockets layer
I/O	input/output
ICMP	internet control message protocol
ICR	intelligent character recognition
IDE	integrated drive electronics
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IIS	Internet Information Services
IMAP	internet mail access protocol
IP	internet protocol
IPCONFIG	internet protocol configuration
IPP	internet printing protocol
IPSEC	internet protocol security
IPX	internetwork packet exchange
IPX/SPX	internetwork packet exchange/sequenced packet exchange
IR	infrared
IrDA	Infrared Data Association
IRQ	interrupt request
ISA	industry standard architecture
ISDN	integrated services digital network

ISO	Industry Standards Organization
ISP	internet service provider
JBOD	just a bunch of disks
Kb	kilobit
KB	Kilobyte or knowledge base
LAN	local area network
LBA	logical block addressing
LC	Lucent connector
LCD	liquid crystal display
LDAP	lightweight directory access protocol
LED	light emitting diode
Li-on	lithium-ion
LPD/LPR	line printer daemon / line printer remote
LPT	line printer terminal
LPT1	line printer terminal 1
LVD	low voltage differential
MAC	media access control / mandatory access control
MAPI	messaging application programming interface
MAU	media access unit, media attachment unit
Mb	megabit
MB	megabyte
MBR	master boot record
MBSA	Microsoft Baseline Security Analyzer
MFD	multi-function device
MFP	multi-function product
MHz	megahertz
MicroDIMM	micro dual inline memory module
MIDI	musical instrument digital interface
MIME	multipurpose internet mail extension
MLI	multiple link interface
MMC	Microsoft management console
MMX	multimedia extensions
MP3	Moving Picture Experts Group Layer 3 Audio
MP4	Moving Picture Experts Group Layer 4
MPEG	Moving Picture Experts Group
MSCONFIG	Microsoft configuration
MSDS	material safety data sheet
MUI	multilingual user interface
NAC	network access control
NAS	network-attached storage
NAT	network address translation
NetBIOS	networked basic input/output system
NetBEUI	networked basic input/output system extended user interface
NFS	network file system
NIC	network interface card
NiCd	nickel cadmium
NiMH	nickel metal hydride
NLX	new low-profile extended
NNTP	network news transfer protocol
NTFS	new technology file system
NTLDR	new technology loader
NTP	Network Time Protocol
OCR	optical character recognition
OEM	original equipment manufacturer
OS	operating system
PAN	personal area network
PATA	parallel advanced technology attachment
PC	personal computer
PCI	peripheral component interconnect
PCle	peripheral component interconnect express
PCIX	peripheral component interconnect extended
PCL	printer control language

PCMCIA	Personal Computer Memory Card International Association
PDA	personal digital assistant
PGA	pin grid array
PGA2	pin grid array 2
PIN	personal identification number
PKI	public key infrastructure
PnP	plug and play
POP3	post office protocol 3
POST	power-on self test
POTS	plain old telephone service
PPP	point-to-point protocol
PPTP	point-to-point tunneling protocol
PRI	primary rate interface
PROM	programmable read-only memory
PS/2	personal system/2 connector
PSTN	public switched telephone network
PSU	power supply unit
PVC	permanent virtual circuit
PXE	preboot execution environment
QoS	quality of service
RAID	redundant array of independent (or inexpensive) discs
RAM	random access memory
RAS	remote access service
RDRAM	RAMBUS® dynamic random access memory
RDP	Remote Desktop Protocol
RF	radio frequency
RFI	radio frequency interference
RGB	red green blue
RIMM	RAMBUS® inline memory module
RIP	routing information protocol
RIS	remote installation service
RISC	reduced instruction set computer
RJ	registered jack
RJ-11	registered jack function 11
RJ-45	registered jack function 45
RMA	returned materials authorization
ROM	read only memory
RS-232(C)	recommended standard 232
RTC	real-time clock
SAN	storage area network
SATA	serial advanced technology attachment
SC	subscription channel
SCP	secure copy protection
SCSI	small computer system interface
SCSI ID	small computer system interface identifier
SD	card secure digital card
SDRAM	synchronous dynamic random access memory
SEC	single edge connector
SFC	system file checker
SGRAM	synchronous graphics random access memory
SIMM	single inline memory module
SLI	scalable link interface or system level integration or scanline interleave mode
S.M.A.R.T.	self-monitoring, analysis, and reporting technology
SMB	server message block or small to midsize business
SMTP	simple mail transport protocol
SNMP	simple network management protocol
SoDIMM	small outline dual inline memory module
SOHO	small office/home office
SP	service pack
SP1	service pack 1
SP2	service pack 2
SP3	service pack 3

SP4	service pack 4
SPDIF	Sony-Philips digital interface format
SPGA	staggered pin grid array
SPX	sequenced package exchange
SRAM	static random access memory
SSH	secure shell
SSID	service set identifier
SSL	secure sockets layer
ST	straight tip
STP	shielded twisted pair
SVGA	super video graphics array
SXGA	super extended graphics array
TB	terabyte
TCP	transmission control protocol
TCP/IP	transmission control protocol/internet protocol
TDR	time domain reflectometer
TFTP	trivial file transfer protocol
TPM	trusted platform module
UAC	user account control
UART	universal asynchronous receiver transmitter
UDF	user defined functions or universal disk format or universal data format
UDMA	ultra direct memory access
UDP	user datagram protocol
UNC	universal naming convention
UPS	uninterruptible power supply
URL	uniform resource locator
USB	universal serial bus
USMT	user state migration tool
UTP	unshielded twisted pair
UXGA	ultra extended graphics array
VESA	Video Electronics Standards Association
VFAT	virtual file allocation table
VGA	video graphics array
VoIP	voice over internet protocol
VPN	virtual private network
VRAM	video random access memory
WAN	wide area network
WAP	wireless application protocol
WEP	wired equivalent privacy
WIFI	wireless fidelity
WINS	windows internet name service
WLAN	wireless local area network
WPA	wireless protected access
WUXGA	wide ultra extended graphics array
XGA	extended graphics array
ZIF	zero-insertion-force
ZIP	zigzag inline package

SUPPLEMENT TWO

CompTIA A+ Practical Application (2009 Edition)

Objectives

Exam Number: 220-702

Introduction

In order to receive CompTIA A+ certification a candidate must pass two exams. The first exam is CompTIA A+ Essentials, exam number 220-701. Objectives for the CompTIA A+ Essentials examination are available at www.comptia.org. The CompTIA A+ 220-702 exam, Practical Application, is the second exam required in order for CompTIA A+ certification candidates to complete their certification in the 2009 Edition of CompTIA A+. The CompTIA A+ Practical Application exam measures the necessary competencies for an entry-level IT professional who has hands-on experience in the lab or the field. Successful candidates will have the skills required to install, configure, upgrade, and maintain PC workstations, the Windows OS and SOHO networks. The successful candidate will utilize troubleshooting techniques and tools to effectively and efficiently resolve PC, OS, and network connectivity issues and implement security practices. Job titles in some organizations which are descriptive of the role of this individual may be: Enterprise technician, IT administrator, field service technician, PC or Support technician, etc. Ideally, the CompTIA A+ Practical Application candidate has already passed the CompTIA A+ Essentials examination.

CompTIA A+ is ISO 17024 Accredited (Personnel Certification Accreditation) and, as such, undergoes regular reviews and updates to the exam objectives. The following CompTIA A+ Practical Application objectives reflect the subject areas in the 2009 Edition of this exam, and result from subject matter expert workshops and industry wide survey results regarding the skills and knowledge required of an entry-level IT professional with some hands-on experience. The percentages in this document represent the relative importance of the subject areas (domains) in the associated body of knowledge, and together establish the foundation for an entry-level IT professional. This examination blueprint includes domain weighting, test objectives, and example content. Example topics and concepts are included to clarify the test objectives and should not be construed as a comprehensive listing of all the content of this examination.

Candidates are encouraged to use this document to guide their studies. The contents of the examination blueprint help prioritize topics and provide a guide of what to expect on the CompTIA A+ Practical Application exam. The table below lists the domains measured by this examination and the extent to which they are represented. The CompTIA A+ Practical Application (2009 Edition) exam is based on these objectives.

Domain	Percentage of Examination
1.0 Hardware	38%
2.0 Operating Systems	34%
3.0 Networking	15%
4.0 Security	13%
Total	100%

****Note:** The lists of examples provided in bulleted format below each objective are not exhaustive lists. Other examples of technologies, processes or tasks pertaining to each objective may also be included on the exam although not listed or covered in this objectives document.

CompTIA is constantly reviewing the content of our exams and updating test questions to be sure our exams are current and the security of the questions is protected. When necessary, we will publish updated exams based on existing exam objectives. Please know that all related exam preparation materials will still be valid.

1.0 Hardware

1.1 Given a scenario, install, configure and maintain personal computer components

- Storage devices
 - HDD
 - SATA
 - PATA
 - Solid state
 - FDD
 - Optical drives
 - CD / DVD / RW / Blu-Ray
 - Removable
 - External
- Motherboards
 - Jumper settings
 - CMOS battery
 - Advanced BIOS settings
 - Bus speeds
 - Chipsets
 - Firmware updates
 - Socket types
 - Expansion slots
 - Memory slots
 - Front panel connectors
 - I/O ports
 - Sound, video, USB 1.1, USB 2.0, serial, IEEE 1394 / Firewire, parallel, NIC, modem, PS/2)
- Power supplies
 - Wattages and capacity
 - Connector types and quantity
 - Output voltage
- Processors
 - Socket types
 - Speed
 - Number of cores
 - Power consumption
 - Cache
 - Front side bus
 - 32bit vs. 64bit
- Memory
- Adapter cards
 - Graphics cards
 - Sound cards
 - Storage controllers
 - RAID cards (RAID array – levels 0,1,5)
 - eSATA cards
 - I/O cards
 - Firewire
 - USB
 - Parallel
 - Serial
 - Wired and wireless network cards
 - Capture cards (TV, video)
 - Media reader
- Cooling systems
 - Heat sinks
 - Thermal compound
 - CPU fans
 - Case fans

1.2 Given a scenario, detect problems, troubleshoot and repair/replace personal computer components

- Storage devices
 - HDD
 - SATA
 - PATA
 - Solid state
 - FDD
 - Optical drives
 - CD / DVD / RW / Blu-Ray
 - Removable
 - External
- Motherboards
 - Jumper settings
 - CMOS battery
 - Advanced BIOS settings
 - Bus speeds
 - Chipsets
 - Firmware updates
 - Socket types
 - Expansion slots
 - Memory slots
 - Front panel connectors
 - I/O ports
 - Sound, video, USB 1.1, USB 2.0, serial, IEEE 1394 / Firewire, parallel, NIC, modem, PS/2)
- Power supplies
 - Wattages and capacity
 - Connector types and quantity
 - Output voltage
- Processors
 - Socket types
 - Speed
 - Number of cores
 - Power consumption
 - Cache
 - Front side bus
 - 32bit vs. 64bit
- Memory
- Adapter cards
 - Graphics cards - memory
 - Sound cards
 - Storage controllers
 - RAID cards
 - eSATA cards
 - I/O cards
 - Firewire
 - USB
 - Parallel
 - Serial
 - Wired and wireless network cards
 - Capture cards (TV, video)
 - Media reader
- Cooling systems
 - Heat sinks
 - Thermal compound
 - CPU fans
 - Case fans

1.3 Given a scenario, install, configure, detect problems, troubleshoot and repair/replace laptop components

- Components of the LCD including inverter, screen and video card

- Hard drive and memory
- Disassemble processes for proper re-assembly
 - Document and label cable and screw locations
 - Organize parts
 - Refer to manufacturer documentation
 - Use appropriate hand tools
- Recognize internal laptop expansion slot types
- Upgrade wireless cards and video card
- Replace keyboard, processor, plastics, pointer devices, heat sinks, fans, system board, CMOS battery, speakers

1.4 Given a scenario, select and use the following tools

- Multimeter
- Power supply tester
- Specialty hardware / tools
- Cable testers
- Loop back plugs
- Anti-static pad and wrist strap
- Extension magnet

1.5 Given a scenario, detect and resolve common printer issues

- Symptoms
 - Paper jams
 - Blank paper
 - Error codes
 - Out of memory error
 - Lines and smearing
 - Garbage printout
 - Ghosted image
 - No connectivity
- Issue resolution
 - Replace fuser
 - Replace drum
 - Clear paper jam
 - Power cycle
 - Install maintenance kit (reset page count)
 - Set IP on printer
 - Clean printer

2.0 Operating Systems - unless otherwise noted, operating systems referred to within include Microsoft Windows 2000, Windows XP Professional, XP Home, XP MediaCenter, Windows Vista Home, Home Premium, Business and Ultimate.

2.1 Select the appropriate commands and options to troubleshoot and resolve problems

- MSCONFIG
- DIR
- CHKDSK (/f /r)
- EDIT
- COPY (/a /v /y)
- XCOPY
- FORMAT
- IPCONFIG (/all /release /renew)
- PING (-t -l)
- MD / CD / RD
- NET
- TRACERT
- NSLOOKUP
- [command name] /?
- SFC

2.2 Differentiate between Windows Operating System directory structures (Windows 2000, XP and Vista)

- User file locations
- System file locations
- Fonts
- Temporary files
- Program files
- Offline files and folders

2.3 Given a scenario, select and use system utilities / tools and evaluate the results

- Disk management tools
 - DEFRAG
 - NTBACKUP
 - Check Disk
- Disk Manager
 - Active, primary, extended and logical partitions
 - Mount points
 - Mounting a drive
 - FAT32 and NTFS
 - Drive status
 - Foreign drive
 - Healthy
 - Formatting
 - Active unallocated
 - Failed
 - Dynamic
 - Offline
 - Online
- System monitor
- Administrative tools
 - Event Viewer
 - Computer Management
 - Services
 - Performance Monitor
- Devices Manager
 - Enable
 - Disable
 - Warnings
 - Indicators

- Task Manager
 - Process list
 - Resource usage
 - Process priority
 - Termination
- System Information
- System restore
- Remote Desktop Protocol (Remote Desktop / Remote Assistance)
- Task Scheduler
- Regional settings and language settings

2.4 Evaluate and resolve common issues

- Operational Problems
 - Windows specific printing problems
 - Print spool stalled
 - Incorrect / incompatible driver / form printing
 - Auto-restart errors
 - Bluescreen error
 - System lock-up
 - Devices drivers failure (input / output devices)
 - Application install, start or load failure
 - Service fails to start
- Error Messages and Conditions
 - Boot
 - Invalid boot disk
 - Inaccessible boot drive
 - Missing NTLDR
 - Startup
 - Device / service failed to start
 - Device / program in registry not found
 - Event viewer (errors in the event log)
 - System Performance and Optimization
 - Aero settings
 - Indexing settings
 - UAC
 - Side bar settings
 - Startup file maintenance
 - Background processes

3.0 Networking

3.1 Troubleshoot client-side connectivity issues using appropriate tools

- TCP/IP settings
 - Gateway
 - Subnet mask
 - DNS
 - DHCP (dynamic vs.static)
 - NAT (private and public)
- Characteristics of TCP/IP
 - Loopback addresses
 - Automatic IP addressing
- Mail protocol settings
 - SMTP
 - IMAP
 - POP
- FTP settings
 - Ports
 - IP addresses
 - Exceptions
 - Programs
- Proxy settings
 - Ports
 - IP addresses
 - Exceptions
 - Programs
- Tools (use and interpret results)
 - Ping
 - Tracert
 - Nslookup
 - Netstat
 - Net use
 - Net /?
 - Ipconfig
 - telnet
 - SSH
- Secure connection protocols
 - SSH
 - HTTPS
- Firewall settings
 - Open and closed ports
 - Program filters

3.2 Install and configure a small office home office (SOHO) network

- Connection types
 - Dial-up
 - Broadband
 - DSL
 - Cable
 - Satellite
 - ISDN
 - Wireless
 - All 802.11
 - WEP
 - WPA
 - SSID
 - MAC filtering
 - DHCP settings
 - Routers / Access Points
 - Disable DHCP
 - Use static IP

- Change SSID from default
 - Disable SSID broadcast
 - MAC filtering
 - Change default username and password
 - Update firmware
 - Firewall
 - LAN (10/100/1000BaseT, Speeds)
 - Bluetooth (1.0 vs. 2.0)
 - Cellular
 - Basic VoIP (consumer applications)
- • Basics of hardware and software firewall configuration
 - Port assignment / setting up rules (exceptions)
 - Port forwarding / port triggering
 - Physical installation
 - Wireless router placement
 - Cable length

4.0 Security

4.1 Given a scenario, prevent, troubleshoot and remove viruses and malware

- Use antivirus software
- Identify malware symptoms
- Quarantine infected systems
- Research malware types, symptoms and solutions (virus encyclopedias)
- Remediate infected systems
- Update antivirus software
 - Signature and engine updates
 - Automatic vs. manual
- Schedule scans
- Repair boot blocks
- Scan and removal techniques
 - Safe mode
 - Boot environment
- Educate end user

4.2 Implement security and troubleshoot common issues

- Operating systems
 - Local users and groups: Administrator, Power Users, Guest, Users
 - Vista User Access Control (UAC)
 - NTFS vs. Share permissions
 - Allow vs. deny
 - Difference between moving and copying folders and files
 - File attributes
 - Shared files and folders
 - Administrative shares vs. local shares
 - Permission propagation
 - Inheritance
 - System files and folders
 - Encryption (Bitlocker, EFS)
 - User authentication
- System
 - BIOS security
 - Drive lock
 - Passwords
 - Intrusion detection
 - TPM

CompTIA A+ Acronyms

Introduction

The following is a list of acronyms which appear on the CompTIA A+ exams. Candidates are encouraged to review the complete list and attain a working knowledge of all listed acronyms as a part of a comprehensive exam preparation program.

ACRONYM SPELLED OUT

AC	alternating current
ACL	access control list
ACPI	advanced configuration and power interface
ACT	activity
ADSL	asymmetrical digital subscriber line
AGP	accelerated graphics port
AMD	advanced micro devices
APIPA	automatic private internet protocol addressing
APM	advanced power management
ARP	address resolution protocol
ASR	automated system recovery
AT	advanced technology
ATA	advanced technology attachment
ATAPI	advanced technology attachment packet interface
ATM	asynchronous transfer mode
ATX	advanced technology extended
BIOS	basic input/output system
BNC	Bayonet-Neill-Concelman or British Naval Connector
BTX	balanced technology extended
CD	compact disc
CD-ROM	compact disc-read-only memory
CD-RW	compact disc-rewritable
CDFS	compact disc file system
CFS	Central File System, Common File System, Command File System
CMOS	complementary metal-oxide semiconductor
COMx	communication port (x=port number)
CPU	central processing unit
CRT	cathode-ray tube
DAC	discretionary access control
DB-25	serial communications D-shell connector, 25 pins
DB-9	9 pin D shell connector
DC	direct current
DDOS	distributed denial of service
DDR	double data-rate
DDR RAM	double data-rate random access memory
DDR SDRAM	double data-rate synchronous dynamic random access memory
DFS	distributed file system
DHCP	dynamic host configuration protocol
DIMM	dual inline memory module
DIN	Deutsche Industrie Norm
DIP	dual inline package
DLT	digital linear tape
DLP	digital light processing
DMA	direct memory access
DMZ	demilitarized zone
DNS	domain name service or domain name server
DOS	denial of service
DPMS	display power management signaling
DRAM	dynamic random access memory
DSL	digital subscriber line
DVD	digital video disc or digital versatile disc
DVD-RAM	digital video disc-random access memory

DVD-ROM	digital video disc-read only memory
DVD-R	digital video disc-recordable
DVD-RW	digital video disc-rewritable
DVI	digital visual interface
ECC	error correction code
ECP	extended capabilities port
EEPROM	electrically erasable programmable read-only memory
EFS	encrypting file system
EIDE	enhanced integrated drive electronics
EMI	electromagnetic interference
EMP	electromagnetic pulse
EPROM	erasable programmable read-only memory
EPP	enhanced parallel port
ERD	emergency repair disk
ESD	electrostatic discharge
EVGA	extended video graphics adapter/array
EVDO	evolution data optimized or evolution data only
FAT	file allocation table
FAT12	12-bit file allocation table
FAT16	16-bit file allocation table
FAT32	32-bit file allocation table
FDD	floppy disk drive
Fn	Function (referring to the function key on a laptop)
FPM	fast page-mode
FRU	field replaceable unit
FSB	Front Side Bus
FTP	file transfer protocol
FQDN	fully qualified domain name
Gb	gigabit
GB	gigabyte
GDI	graphics device interface
GHz	gigahertz
GUI	graphical user interface
GPS	global positioning system
GSM	global system for mobile communications
HAL	hardware abstraction layer
HCL	hardware compatibility list
HDD	hard disk drive
HDMI	high definition media interface
HPFS	high performance file system
HTML	hypertext markup language
HTTP	hypertext transfer protocol
HTTPS	hypertext transfer protocol over secure sockets layer
I/O	input/output
ICMP	internet control message protocol
ICR	intelligent character recognition
IDE	integrated drive electronics
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IIS	Internet Information Services
IMAP	internet mail access protocol
IP	internet protocol
IPCONFIG	internet protocol configuration
IPP	internet printing protocol
IPSEC	internet protocol security
IPX	internetwork packet exchange
IPX/SPX	internetwork packet exchange/sequenced packet exchange
IR	infrared
IrDA	Infrared Data Association
IRQ	interrupt request
ISA	industry standard architecture
ISDN	integrated services digital network

ISO	Industry Standards Organization
ISP	internet service provider
JBOD	just a bunch of disks
Kb	kilobit
KB	Kilobyte or knowledge base
LAN	local area network
LBA	logical block addressing
LC	Lucent connector
LCD	liquid crystal display
LDAP	lightweight directory access protocol
LED	light emitting diode
Li-on	lithium-ion
LPD/LPR	line printer daemon / line printer remote
LPT	line printer terminal
LPT1	line printer terminal 1
LVD	low voltage differential
MAC	media access control / mandatory access control
MAPI	messaging application programming interface
MAU	media access unit, media attachment unit
Mb	megabit
MB	megabyte
MBR	master boot record
MBSA	Microsoft Baseline Security Analyzer
MFD	multi-function device
MFP	multi-function product
MHz	megahertz
MicroDIMM	micro dual inline memory module
MIDI	musical instrument digital interface
MIME	multipurpose internet mail extension
MLI	multiple link interface
MMC	Microsoft management console
MMX	multimedia extensions
MP3	Moving Picture Experts Group Layer 3 Audio
MP4	Moving Picture Experts Group Layer 4
MPEG	Moving Picture Experts Group
MSCONFIG	Microsoft configuration
MSDS	material safety data sheet
MUI	multilingual user interface
NAC	network access control
NAS	network-attached storage
NAT	network address translation
NetBIOS	networked basic input/output system
NetBEUI	networked basic input/output system extended user interface
NFS	network file system
NIC	network interface card
NiCd	nickel cadmium
NiMH	nickel metal hydride
NLX	new low-profile extended
NNTP	network news transfer protocol
NTFS	new technology file system
NTLDR	new technology loader
NTP	Network Time Protocol
OCR	optical character recognition
OEM	original equipment manufacturer
OS	operating system
PAN	personal area network
PATA	parallel advanced technology attachment
PC	personal computer
PCI	peripheral component interconnect
PCle	peripheral component interconnect express
PCIX	peripheral component interconnect extended
PCL	printer control language

PCMCIA	Personal Computer Memory Card International Association
PDA	personal digital assistant
PGA	pin grid array
PGA2	pin grid array 2
PIN	personal identification number
PKI	public key infrastructure
PnP	plug and play
POP3	post office protocol 3
POST	power-on self test
POTS	plain old telephone service
PPP	point-to-point protocol
PPTP	point-to-point tunneling protocol
PRI	primary rate interface
PROM	programmable read-only memory
PS/2	personal system/2 connector
PSTN	public switched telephone network
PSU	power supply unit
PVC	permanent virtual circuit
PXE	preboot execution environment
QoS	quality of service
RAID	redundant array of independent (or inexpensive) discs
RAM	random access memory
RAS	remote access service
RDRAM	RAMBUS® dynamic random access memory
RDP	Remote Desktop Protocol
RF	radio frequency
RFI	radio frequency interference
RGB	red green blue
RIMM	RAMBUS® inline memory module
RIP	routing information protocol
RIS	remote installation service
RISC	reduced instruction set computer
RJ	registered jack
RJ-11	registered jack function 11
RJ-45	registered jack function 45
RMA	returned materials authorization
ROM	read only memory
RS-232(C)	recommended standard 232
RTC	real-time clock
SAN	storage area network
SATA	serial advanced technology attachment
SC	subscription channel
SCP	secure copy protection
SCSI	small computer system interface
SCSI ID	small computer system interface identifier
SD	card secure digital card
SDRAM	synchronous dynamic random access memory
SEC	single edge connector
SFC	system file checker
SGRAM	synchronous graphics random access memory
SIMM	single inline memory module
SLI	scalable link interface or system level integration or scanline interleave mode
S.M.A.R.T.	self-monitoring, analysis, and reporting technology
SMB	server message block or small to midsize business
SMTP	simple mail transport protocol
SNMP	simple network management protocol
SoDIMM	small outline dual inline memory module
SOHO	small office/home office
SP	service pack
SP1	service pack 1
SP2	service pack 2
SP3	service pack 3

SP4	service pack 4
SPDIF	Sony-Philips digital interface format
SPGA	staggered pin grid array
SPX	sequenced package exchange
SRAM	static random access memory
SSH	secure shell
SSID	service set identifier
SSL	secure sockets layer
ST	straight tip
STP	shielded twisted pair
SVGA	super video graphics array
SXGA	super extended graphics array
TB	terabyte
TCP	transmission control protocol
TCP/IP	transmission control protocol/internet protocol
TDR	time domain reflectometer
TFTP	trivial file transfer protocol
TPM	trusted platform module
UAC	user account control
UART	universal asynchronous receiver transmitter
UDF	user defined functions or universal disk format or universal data format
UDMA	ultra direct memory access
UDP	user datagram protocol
UNC	universal naming convention
UPS	uninterruptible power supply
URL	uniform resource locator
USB	universal serial bus
USMT	user state migration tool
UTP	unshielded twisted pair
UXGA	ultra extended graphics array
VESA	Video Electronics Standards Association
VFAT	virtual file allocation table
VGA	video graphics array
VoIP	voice over internet protocol
VPN	virtual private network
VRAM	video random access memory
WAN	wide area network
WAP	wireless application protocol
WEP	wired equivalent privacy
WIFI	wireless fidelity
WINS	windows internet name service
WLAN	wireless local area network
WPA	wireless protected access
WUXGA	wide ultra extended graphics array
XGA	extended graphics array
ZIF	zero-insertion-force
ZIP	zigzag inline package

SUPPLEMENT THREE

CompTIA Network+ (2009 Edition) Certification Examination Objectives INTRODUCTION

The CompTIA Network+ (2009 Edition) certification is an internationally recognized validation of the technical knowledge required of foundation-level IT network practitioners.

The CompTIA Network+ (2009 Edition) certification ensures that the successful candidate has the important knowledge and skills necessary to manage, maintain, troubleshoot, install, operate and configure basic network infrastructure, describe networking technologies, basic design principles, and adhere to wiring standards and use testing tools.

The skills and knowledge measured by this examination were derived from an industry-wide job task analysis and validated through an industry-wide global survey in Q2 2008. The results of this survey were used in weighing the domains and ensuring that the weighting is representative of the relative importance of the content.

It is recommended for CompTIA Network+ (2009 Edition) candidates to have the following:

- CompTIA A+ certification or equivalent knowledge, though CompTIA A+ certification is not required.
- Have at least 9 to 12 months of work experience in IT networking.

The table below lists the domains measured by this examination and the extent to which they are represented. CompTIA Network+ (2009 Edition) exams are based on these objectives.

Domain	Percentage of Examination
1.0 Network Technologies	20%
2.0 Network Media and Topologies	20%
3.0 Network Devices	17%
4.0 Network Management	20%
5.0 Network Tools	12%
6.0 Network Security	11%
Total	100%

****Note:** The bulleted lists below each objective are not exhaustive lists. Even though they are not included in this document, other examples of technologies, processes or tasks pertaining to each objective may also be included on the exam.

(A list of acronyms used in these objectives appears at the end of this document.)

1.0 Network Technologies

1.1 Explain the function of common networking protocols

- TCP
- FTP
- UDP
- TCP/IP suite
- DHCP
- TFTP
- DNS
- HTTP(S)
- ARP
- SIP (VoIP)
- RTP (VoIP)
- SSH
- POP3
- NTP
- IMAP4
- Telnet
- SMTP
- SNMP2/3
- ICMP
- IGMP
- TLS

1.2 Identify commonly used TCP and UDP default ports

- TCP ports
- FTP – 20, 21
- SSH – 22
- TELNET – 23
- SMTP – 25
- DNS – 53
- HTTP – 80
- POP3 – 110
- NTP – 123
- IMAP4 – 143
- HTTPS – 443
- UDP ports
- TFTP – 69
- DNS – 53
- BOOTPS/DHCP – 67
- SNMP – 161

1.3 Identify the following address formats

- IPv6
- IPv4
- MAC addressing

1.4 Given a scenario, evaluate the proper use of the following addressing technologies and addressing schemes

- Addressing Technologies
 - Subnetting
 - Classful vs. classless (e.g. CIDR, Supernetting)
 - NAT
 - PAT
 - SNAT
 - Public vs. private
 - DHCP (static, dynamic APIPA)
- Addressing schemes
 - Unicast

- Multicast
- Broadcast

1.5 Identify common IPv4 and IPv6 routing protocols

- Link state
 - OSPF
 - IS-IS
- Distance vector
 - RIP
 - RIPv2
 - BGP
- Hybrid
 - EIGRP

1.6 Explain the purpose and properties of routing

- IGP vs. EGP
- Static vs. dynamic
- Next hop
- Understanding routing tables and how they pertain to path selection
- Explain convergence (steady state)

1.7 Compare the characteristics of wireless communication standards

- 802.11 a/b/g/n
 - Speeds
 - Distance
 - Channels
 - Frequency
- Authentication and encryption
 - WPA
 - WEP
 - RADIUS
 - TKIP
 -

2.0 Network Media and Topologies

2.1 Categorize standard cable types and their properties

- Type:
 - CAT3, CAT5, CAT5e, CAT6
 - STP, UTP
 - Multimode fiber, single-mode fiber
 - Coaxial
 - RG-59
 - RG-6
 - Serial
 - Plenum vs. Non-plenum
- Properties:
 - Transmission speeds
 - Distance
 - Duplex
 - Noise immunity (security, EMI)
 - Frequency

2.2 Identify common connector types

- RJ-11
- J-45
- BNC
- SC
- ST
- LC
- RS-232

2.3 Identify common physical network topologies

- Star
- Mesh
- Bus
- Ring
- Point to point
- Point to multipoint
- Hybrid

2.4 Given a scenario, differentiate and implement appropriate wiring standards

- 568A
- 568B
- Straight vs. cross-over
- Rollover
- Loopback

2.5 Categorize WAN technology types and properties

- Type:
 - Frame relay
 - 1/T1
 - ADSL
 - SDSL
 - VDSL
 - Cable modem
 - Satellite
 - E3/T3
 - OC-x
 - Wireless
 - ATM
 - SONET
 - MPLS
 - ISDN BRI
 - ISDN PRI

- POTS
- PSTN
- Properties
 - Circuit switch
 - Packet switch
 - Speed
 - Transmission media
 - Distance

2.6 Categorize LAN technology types and properties

- Types:
 - Ethernet
 - 10BaseT
 - 100BaseTX
 - 100BaseFX
 - 1000BaseT
 - 1000BaseX
 - 10GBaseSR
 - 10GBaseLR
 - 10GBaseER
 - 10GBaseSW
 - 10GBaseLW
 - 10GBaseEW
 - 10GBaseT

2.7 Explain common logical network topologies and their characteristics

- Peer to peer
- Client/server
- VPN
- VLAN

2.8 Install components of wiring distribution

- Vertical and horizontal cross connects
- Patch panels
- 66 block
- MDFs
- IDFs
- 25 pair
- 100 pair
- 110 block
- Demarc
- Demarc extension
- Smart jack
- Verify wiring installation
- Verify wiring termination

3.0 Network Devices

3.1 Install, configure and differentiate between common network devices

- Hub
- Repeater
- Modem
- NIC
- Media converters
- Basic switch
- Bridge
- Wireless access point
- Basic router
- Basic firewall
- Basic DHCP server

3.2 Identify the functions of specialized network devices

- Multilayer switch
- Content switch
- DS/IPS
- Load balancer
- Multifunction network devices
- DNS server
- Bandwidth shaper
- Proxy server
- CSU/DSU

3.3 Explain the advanced features of a switch

- PoE
- Spanning tree
- LAN
- Trunking
- Port mirroring
- Port authentication

3.4 Implement a basic wireless network

- Install client
- Access point placement
- Install access point
 - Configure appropriate encryption
 - Configure channels and frequencies
 - Set ESSID and beacon
- Verify installation

4.0 Network Management

- 4.1 Explain the function of each layer of the OSI model**
- Layer 1 – physical
 - Layer 2 – data link
 - Layer 3 – network
 - Layer 4 – transport
 - Layer 5 – session
 - Layer 6 – presentation
 - Layer 7 – application
- 4.2 Identify types of configuration management documentation**
- Wiring schematics
 - Physical and logical network diagrams
 - Baselines
 - Policies, procedures and configurations
 - Regulations
- 4.3 Given a scenario, evaluate the network based on configuration management documentation**
- Compare wiring schematics, physical and logical network diagrams, baselines, policies and procedures and configurations to network devices and infrastructure
 - Update wiring schematics, physical and logical network diagrams, configurations and job logs as needed
- 4.4 Conduct network monitoring to identify performance and connectivity issues using the following:**
- Network monitoring utilities (e.g. packet sniffers, connectivity software, load testing, throughput testers)
 - System logs, history logs, event logs
- 4.5 Explain different methods and rationales for network performance optimization**
- Methods:
 - QoS
 - Traffic shaping
 - Load balancing
 - High availability
 - Caching engines
 - Fault tolerance
 - Reasons:
 - • Latency sensitivity
 - • High bandwidth applications
 - ○ VoIP
 - ○ Video applications
 - • Uptime
- 4.6 Given a scenario, implement the following network troubleshooting methodology**
- Information gathering – identify symptoms and problems
 - Identify the affected areas of the network
 - Determine if anything has changed
 - Establish the most probable cause
 - Determine if escalation is necessary
 - Create an action plan and solution identifying potential effects
 - Implement and test the solution
 - Identify the results and effects of the solution
 - Document the solution and the entire process
- 4.7 Given a scenario, troubleshoot common connectivity issues and select an appropriate solution**
- Physical issues:
 - Cross talk
 - Near End crosstalk
 - Attenuation

- Collisions
- Shorts
- Open
- Impedance mismatch (echo)
- Interference
- Logical issues:
 - • Port speed
 - • Port duplex mismatch
 - • Incorrect VLAN
 - • Incorrect IP address
 - • Wrong gateway
 - • Wrong DNS
 - • Wrong subnet mask
 - Issues that should be identified but escalated:
 - Switching loop
 - Routing loop
 - Route problems
 - Proxy arp
 - Broadcast storms
 - Wireless Issues:
 - Interference (bleed, environmental factors)
 - Incorrect encryption
 - Incorrect channel
 - Incorrect frequency
 - ESSID mismatch
 - Standard mismatch (802.11 a/b/g/n)
 - Distance
 - Bounce
 - Incorrect antenna placement

5.0 Network Tools

5.1 **Given a scenario, select the appropriate command line interface tool and interpret the output to verify functionality**

- Traceroute
- Ipconfig
- fconfig
- Ping
- Arp ping
- Arp
- Nslookup
- Hostname
- Dig
- Mtr
- Route
- Nbtstat
- Netstat

5.2 **Explain the purpose of network scanners**

- Packet sniffers
- Intrusion detection software
- Intrusion prevention software
- Port scanners

5.3 **Given a scenario, utilize the appropriate hardware tools**

- Cable testers
- Protocol analyzer
- Certifiers
- TDR
- TDR
- Multimeter
- Toner probe
- Butt set
- Punch down tool
- Cable stripper
- Snips
- Voltage event recorder
- Temperature monitor

6.0 Network Security

6.1 Explain the function of hardware and software security devices

- Network based firewall
- Host based firewall
- IDS
- PS
- VPN concentrator

6.2 Explain common features of a firewall

- Application layer vs. network layer
- Stateful vs. stateless
- Scanning services
- Content filtering
- Signature identification
- Zones

6.3 Explain the methods of network access security

- Filtering:
 - • ACL
 - ◦ MAC filtering
 - ◦ IP filtering
 - • Tunneling and encryption
 - ◦ SSL VPN
 - ◦ VPN
 - ◦ L2TP
 - ◦ PPTP
 - ◦ IPSEC
 - • Remote access
 - ◦ RAS
 - ◦ RDP
 - ◦ PPPoE
 - ◦ PPP
 - ◦ VNC
 - ◦ ICA

6.4 Explain methods of user authentication

- • PKI
- • Kerberos
- • AAA
 - ◦ RADIUS
 - ◦ TACACS+
- • Network access control
 - ◦ 802.1x
- • CHAP
- • MS-CHAP
- • EAP

6.5 Explain issues that affect device security

- • Physical security
- • Restricting local and remote access
- • Secure methods vs. unsecure methods
 - ◦ SSH, HTTPS, SNMPv3, SFTP, SCP
 - ◦ TELNET, HTTP, FTP, RSH, RCP, SNMPv1/2

6.6 Identify common security threats and mitigation techniques

- Security threats
 - DoS
 - Viruses
 - Worms
 - Attackers

- Man in the middle
 - murf
 - Rogue access points
 - Social engineering (phishing)
- Mitigation techniques
 - Policies and procedures
 - User training

NETWORK+ ACRONYMS

AAA	Authentication Authorization and Accounting
ACL	Access Control List
ADF	Automatic Document Feeder
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
AEP	American Electric Power
AFP	AppleTalk Filing Protocol
AH	Authentication Header
AM	Amplitude Modulation
AMI	Alternate Mark Inversion
APIPA	Automatic Private Internet Protocol Addressing
ARIN	American Registry for Internet Numbers
ARP	Address Resolution Protocol
ASP	Application Service Provider
ATM	Asynchronous Transfer Mode
BDF	Building Distribution Frame
BERT	Bit-Error Rate Test
BGP	Border Gateway Protocol
BNC	British Naval Connector / Bayonet Niell-Concelman
BootP	Boot Protocol /Bootstrap Protocol
BPDU	Bridge Protocol Data Unit
BRI	Basic Rate Interface
CHAP	Challenge Handshake Authentication Protocol
CIDR	Classless inter domain routing
CNAME	Canonical Name
CRAM-MD5	Challenge-Response Authentication Mechanism – Message Digest 5
CSMA / CA	Carrier Sense Multiple Access / Collision Avoidance
CSMA / CD	Carrier Sense Multiple Access / Collision Detection
CSU	Channel Service Unit
dB	decibels
DHCP	Dynamic Host Configuration Protocol
DLC	Data Link Control
DMZ	Demilitarized Zone
DNS	Domain Name Service / Domain Name Server / Domain Name System
DOCSIS	Data-Over-Cable Service Interface Specification
DoS	Denial of Service
DDoS	Distributed Denial of Service
DSL	Digital Subscriber Line
DSU	Data Service Unit
DWDM	Dense Wavelength Division Multiplexing
E1	E-Carrier Level 1
EAP	Extensible Authentication Protocol
EGP	Exterior Gateway Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
EMI	Electromagnetic Interference
ESD	Electrostatic Discharge
ESSID	Extended Service Set Identifier
ESP	Encapsulated security packets
FDDI	Fiber Distributed Data Interface
FDM	Frequency Division Multiplexing
FHSS	Frequency Hopping Spread Spectrum
FM	Frequency Modulation
FQDN	Fully Qualified Domain Name / Fully Qualified Distinguished Name
FTP	File Transfer Protocol
GBIC	Gigabit Interface Converter
Gbps	Giga bits per second
HDLC	High-Level Data Link Control
HSRP	Hot Standby Router Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure

Hz	Hertz
IANA	Internet Assigned Numbers Authority
ICA	Independent Computer Architecture
ICANN	Internet Corporation for Assigned Names and Numbers
ICMP	Internet Control Message Protocol
ICS	Internet Connection Sharing
IDF	Intermediate Distribution Frame
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Multicast Protocol
IGP	Interior Gateway Protocol
IIS	Internet Information Services
IKE	Internet Key Exchange
IMAP4	Internet Message Access Protocol version 4
InterNIC	Internet Network Information Center
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPX	Internetwork Packet Exchange
ISDN	Integrated Services Digital Network
IS-IS	Intermediate System - Intermediate system
ISP	Internet Service Provider
IT	Information Technology
Kbps	Kilobits per second
L2F	Layer 2 Forwarding
L2TP	Layer 2 Tunneling Protocol
LACP	Link aggregation control protocol
LAN	Local Area Network
LC	Local Connector
LDAP	Lightweight Directory Access Protocol
LEC	Local Exchange Carrier
LED	Light Emitting Diode
LLC	Logical Link Control
LPR	Line Printer Request
MAC	Media Access Control / Medium Access Control
Mbps	Megabits per second
MBps	Megabytes per second
MDF	Main Distribution Frame
MDI	Media Dependent Interface
MDIX	Media Dependent Interface Crossover
MIB	Management Information Base
MMF	Multimode Fiber
MPLS	Multi-Protocol Label Switching
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol
MT-RJ	Mechanical Transfer-Registered Jack
MX	Mail Exchanger
NAC	Network Access Control
NAT	Network Address Translation
NCP	Network Control Protocol
NetBEUI	Network Basic Input / Output Extended User Interface
NetBIOS	Network Basic Input / Output System
NFS	Network File Service
NIC	Network Interface Card
nm	Nanometer
NNTP	Network News Transport Protocol
NTP	Network Time Protocol
NWLINK	Microsoft IPX/SPX Protocol
OCx	Optical Carrier
OS	Operating Systems
OSI	Open Systems Interconnect

OSPF	Open Shortest Path First
OTDR	Optical Time Domain Reflectometer
PAP	Password Authentication Protocol
PAT	Port Address Translation
PC	Personal Computer
PKI	Public Key Infrastructure
PoE	Power over Ethernet
POP3	Post Office Protocol version 3
POTS	Plain Old Telephone System
PPP	Point-to-Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
PPTP	Point-to-Point Tunneling Protocol
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
PVC	Permanent Virtual Circuit
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RARP	Reverse Address Resolution Protocol
RAS	Remote Access Service
RDP	Remote Desktop Protocol
RFI	Radio Frequency Interface
RG	Radio Guide
RIP	Routing Internet Protocol
RJ	Registered Jack
RSA	Rivest, Shamir, Adelman
RSH	Remote Shell
RTP	Real Time Protocol
SC	Standard Connector / Subscriber Connector
SCP	Secure Copy Protocol
SDSL	Symmetrical Digital Subscriber Line
SFTP	Secure File Transfer Protocol
SIP	Session Initiation Protocol
SLIP	Serial Line Internet Protocol
SMF	Single Mode Fiber
SMTp	Simple Mail Transfer Protocol
SNAT	Static Network Address Translation
SNMP	Simple Network Management Protocol
SOA	Start of Authority
SOHO	Small Office / Home Office
SONET	Synchronous Optical Network
SPS	Standby Power Supply
SPX	Sequenced Packet Exchange
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
ST	Straight Tip
STP	Shielded Twisted Pair
T1	T-Carrier Level 1
TA	Terminal Adaptor
TACACS+	Terminal Access Control Access Control System+
TCP	Transmission Control Protocol
TCP / IP	Transmission Control Protocol / Internet Protocol
tcsh	Turbo C shell
TDM	Time Division Multiplexing
TDR	Time Domain Reflectometer
Telco	Telephone Company
TFTP	Trivial File Transfer Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTL	Time to Live
UDP	User Datagram Protocol
UNC	Universal Naming Convention

UPS	Uninterruptible Power Supply
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTP	Unshielded Twisted Pair
VDSL	Variable Digital Subscriber Line
VLAN	Virtual Local Area Network
VNC	Virtual Network Connection
VoIP	Voice over IP
VPN	Virtual Private Network
VTP	Virtual Trunk Protocol
WAN	Wide Area Network
WAP	Wireless Application Protocol / Wireless Access Point
WEP	Wired Equivalent Privacy
WINS	Window Internet Name Service
WPA	Wi-Fi Protected Access
www	World Wide Web
X.25	CCITT Packet Switching Protocol
XML	eXtensible Markup Language
XDSL	Extended Digital Subscriber Line
Zeroconf	Zero Configuration