REQUEST FOR PROPOSALS

NUMBER NS-49-12

2012 NKU IT Security and Network Audit

2012 NKU IT

RFP

SECURITY & NETWORK AUDIT

June 22, 2012

NOTICE OF RFP OPPORTUNITY

BRIEF SCOPE OF WORK:

The purpose of the internal assessment is to test the targeted network's ability to withstand attack inside the network perimeter, and an analysis of potential vulnerabilities that could result from poor or improper system configuration, both known and unknown hardware or software flaws, or operational weaknesses in process, infrastructure, reporting, logging and preventative measures. The overall objectives are to identify potential vulnerabilities within the internal network and identify weaknesses within network controls, reporting, logging, and to prevent and/or detect their exploitation by a hacker/malicious employee/contractor who may obtain access to information resources, cause system disruption or a system outage. Audit tests would need to be performed at times that are conducive to NKU academic and business schedules, such as maintenance windows.

PROJECT TIMETABLE*:*

Invitation for Bid Issued	**Friday, June 22, 2012**
Last Date for Questions	**Wednesday, July 11, 2012 at 4:30 Noon EDT**
Addenda Issued (if applicable)	**Friday, July 13, 2012 at 12:00 Noon EDT**
BIDS DUE	**Friday, July 19, 2012 at 2:00 pm EDT**
Award Bid	**Approximately July 31, 2012 at 4:30 pm**

SUBMISSION:

The bidder shall submit, by the time and date specified via US Postal Service, courier or other delivery service, its bid response in a **sealed package** addressed to:

Jeff Strunk, CPPO
Director of Procurement Services
Lucas Administrative Center, Suite 617
1 Nunn Drive
Northern Kentucky University
Highland Heights, KY 41099

CONTACT FOR PROPOSAL PACKAGE

RFP Package may be downloaded from Procurement Services Website:
http://procurement.nku.edu/bid--quotes---rfps.html

If you have downloaded this Request for Proposal, please contact Eli Baird so that you can be added to the planholders list and notified if there are any addenda.

Eli Baird
Procurement Services, Bid Specialist
Northern Kentucky University
Lucas Administrative Center, 617
Highland Heights, KY 41099
Phone: 859.572.5266
FAX: 859.572.6995
E-mail: bairde1@nku.edu

Information relative to this project obtained from other sources, including other university administration, faculty or staff may not be accurate, will not be considered binding and could adversely affect the potential for selection of your proposal. All requests for additional information and all questions should be directed to Eli Baird, Procurement Services: Bairde1@nku.edu.

Both inner and outer envelopes/packages should bear respondent's name and address, and clearly marked on package(s) as follows:

RFP NS-49-12
2012 NKU IT SECURITY & NETWORK AUDIT

Note: Proposals received after the closing date and time will not be considered.

GENERAL SCOPE OF WORK

2012 NKU IT Security and Network Audit

Objectives of the Security and Network Audit

1. Identification of security vulnerabilities for Northern Kentucky University.
2. Requirements and analysis performed to increase overall security.
3. Perform penetration testing that assists with regulatory compliance standards
4. Identification and prioritization of risks to the University, with suggestions for risk mitigation and security improvements.

NKU personnel will be available to answer questions about the network and server architecture, as well as current security procedures and controls. This will allow the auditor to attempt penetration with full knowledge. Specific Rules of Engagement and the Audit Plan will exist to ensure desired coverage is accomplished. The project manager will monitor the engagement to ensure that the Rules of Engagement are followed and the objectives in the detailed audit plan developed in the audit are met.

The audit and testing should be performed in such a way that NKU business and services are not affected or disrupted in any way.

Section I: Internal Assessment

Objectives: The purpose of the internal assessment is to test the targeted network's ability to withstand attack inside the network perimeter, and an analysis of potential vulnerabilities that could result from poor or improper system configuration, both known and unknown hardware or software flaws, or operational weaknesses in process, infrastructure, reporting, logging and preventative measures. The overall objectives are to identify potential vulnerabilities within the internal network and identify weaknesses within network controls, reporting, logging, and to prevent and/or detect their exploitation by a hacker/malicious employee/contractor who may obtain access to information resources, cause system disruption or a system outage. At a minimum, the audit should include:

- Network Discovery: Ascertain the internal network topology or footprint that provides a map of the critical access paths/points and devices including their Internet protocol (IP) address ranges.
- Vulnerability Analysis: Once critical points/devices are identified within the network, attack those devices given the various types of known vulnerabilities within the system and operating software running on the devices.
- Exploitation: Determine the level of attack that NKU desires and approves, assuring no disruption of systems or services during the tests. Determine the level of attack based on the level of access obtained on the open ports and the target hosts identified by the discovery and analysis stages, or on the basis of information provided by NKU.
    - From an on-site location, attempt to penetrate the internal network.
    - Members of the penetration team connect to the NKU's internal network and attempt to compromise the servers, workstations, and routers.
    - Using compromised accounts, the penetration team uses a series of exploits to attempt to gain root or administrative access to servers, network equipment and other machines in the network. The penetration team identifies the damage that can be done (places files, harvests files, etc.) once root is captured on any of these machines.
    - Once the penetration team captures root on one machine, attempt attacks on other machines in the network from compromised computer. Document all machines they are able to access, the type of capabilities they gained, and harvest some files to prove access.
    - Using the root capabilities on a machine within the network, the penetration team attacks the firewall and Internet connections from the inside.
    - Notify NKU if access level is achieved
    - Record all vulnerabilities noted and provide to NKU for immediate follow-up at the conclusion of the penetration test/vulnerability analysis.
    - Any entry points discovered by the tests are documented. The entry points are exploited in an attempt to penetrate the network
- Intrusion detection response (including logs) reviewed and assessed.

- Perform a review of network logs and available reporting, and report weaknesses as well as improvement opportunities for logging, reporting tools and detection techniques (as a future replacement for current reporting tool - MARS).

Section II: Physical Security

Objectives: Physical Security factors should be evaluated for physically safety and security. Factors to be considered include, but are not limited to:

- Review of the equipment safety and protection from physical elements such as dust, water, temperature controls, and other physical factors.
- Review location of critical equipment - secure, locked, and isolated from access and limited to authorized staff.
- Review of power and emergency (fire, heat, water) protection.
- Report of physical vulnerabilities - prioritized and documented, along with suggestions for improvements.

Section III: Wireless Assessment

Objectives: The purpose of the wireless assessment is to test its ability to withstand attack. The overall objective is to identify potential vulnerabilities within the wireless network and weaknesses in controls in place to prevent and/or detect their exploitation by a hacker/malicious employee/contractor who may obtain access to information resources, cause system disruption or a system outage. At a minimum, the audit objectives must include:

- Network Discovery: Ascertain the internal network topology or footprint that provides a map of the critical access paths/points and devices including their Internet protocol (IP) address ranges.
- Vulnerability Analysis: Once critical points/devices are identified within the network, attack those devices given the various types of known vulnerabilities within the system and operating software running on the devices.
- Exploitation: Determine the level of attack that NKU desires and approves, assuring no disruption of systems or services. Determine the level of attack based on the level of access obtained on the open ports and the target hosts identified by the discovery and analysis stages, or on the basis of information provided by NKU.
    - From an on-site location, attempt to penetrate the internal network.
    - Members of the penetration team connect to the NKU's internal network and attempt to compromise the servers, workstations, and routers.
    - Using compromised accounts, the penetration team uses a series of exploits to attempt to gain root or administrative access to servers, network equipment and other machines in the network. The penetration team identifies the damage that can be done (places files, harvests files, etc.) once root is captured on any of these machines.
    - Once the penetration team captures root on one machine, attempt attacks on other machines in the network from compromised computer. Document all machines they are able to access, the type of capabilities they gained, and harvest some files to prove access.
    - Using the root capabilities on a machine within the network, the penetration team attacks the firewall and Internet connections from the inside.
    - Notify NKU if access level is achieved
    - Record all vulnerabilities noted and provide to NKU for immediate follow-up at the conclusion of the penetration test/vulnerability analysis.
    - Any entry points discovered by the tests are documented. The entry points are exploited in an attempt to penetrate the network
- Intrusion detection response (including logs) reviewed and assessed.
- Perform a review of all network logs and available reporting, and report weaknesses as well as improvement opportunities for logging and reporting tools and detection techniques (as a future replacement for MARS)
    - Recommendations should be vendor independent and should support the current NKU architecture
    - Recommendations should be a minimum of 3 tool(s) or reporting systems.

Section IV: Internet Assessment & Web Assessment

Audit Objectives. The purpose of the Internet assessment is to test the targeted network for vulnerability analysis and exploitation via the Internet. The test methodology allow for a systematic checking for known vulnerabilities and pursuit of potential security risks.

At a minimum, the audit objectives should include: vulnerability analysis and exploitation. Methodology to include but not inclusively defined:

- From a remote (non-NKU) site, attempt penetration from the Internet.
- A determined Internet attack from multiple locations over an extended period is launched.
- Any weaknesses identified are exploited using non-invasive techniques to harvest files, insert files into the network (simple text files) and hop between servers to compile a network diagram and document additional exploits.
- The firewall is to be tested. In addition to non-invasive techniques, techniques that are designed to momentarily disable the firewall are used if it was improperly configured.
- The VPN is to be tested for security and connectivity/remote access.
- NKU's wireless local area network will be tested for secure configuration including but not limited to rogue access points, encryption strength, access rights and coverage leakage.
- Using common hacking methods (such as cross site scripting, SQL injection) try to gain access to private data or deface 5 different service websites ('Find it', Student Email Login, Password Change Page, myNKU and www). Also identify potential weaknesses in web code design on these pages.

Deliverables

The purpose of the audit is to report security improvements, to identify the weaknesses, develop NKU-specific recommendations to address weaknesses, and communicate results to NKU. The final deliverable will be defined prior to engagement, to include the following:

- All observations will be thoroughly discussed with appropriate and related IT management before finalization report
- Include an executive summary and overview
- A presentation to technical and security staff
- Schedule and prioritization of actions based on risk to the university
- Summary of reviewed policies and procedures with recommendation for changes, additions, or deletions
- Compliance standard recommendations for periodic penetration tests
- Additional technical detail will be available as support information to answer questions
- Identification of tests, tools used and results of tests
- Specific gaps, deficiencies, vulnerabilities observed
- In addition to the assessment and findings, make specific recommendations as to how findings can be remedied
- List of vulnerabilities penetrated
- Detailed analysis of strengths and weaknesses
- Recommendations for a continuous audit approach
- Details per the assessment sections as follows:

  Section I: Internal Assessment Specifics
  - Review of architecture/topology of routers and switches
  - Servers
    - Active Directory
    - E-mail
    - Patch Management
    - Compliance standards
  - Recommendations for improvements and course of action
  - Recommendations for logging, reporting, and Intrusion Detection system

  Section II: Physical Assessment Specifics
  - Location reviews, device hardening improvements
  - Employee Access reviews

- Environmental (fire, water, dust, physical) reviews
- Recommendations for improvements and course of action

Section III: Wireless Assessment Specifics

- Review of wireless current and future wireless goals, objectives
- Growth path to ensure security and growth as needed for current and future mobility across campus
- Recommendations for improvements and course of action

Section IV: Internet Assessment Specifics

- Review and analysis of VPN Security
  - Site to Site Tunnels
  - Remote Access
- Review of firewall security
  - Design and Architecture
  - Identification of gaps in access list
- Vulnerability of all Internet accessible hosts, websites, and application coding.
- Recommendations to reduce web vulnerabilities and improve development coding methods.

A presentation to an executive group that would entail a summary of results with actual examples to illustrate points may be required. The presentation will include descriptions of methodologies be kept very brief with the focus on the overall level of risk within the network and the types of actions that will be necessary to reduce risk to acceptable levels. Descriptions of the types of vulnerabilities may be used, but where possible, specific system identification will be avoided to prevent the focus from being diverted from larger problems to more specific and familiar system-specific problems. The presentations, as well as the final report itself, must be written to identify the weaknesses and lay out a roadmap to mitigate unnecessary risk in the network, and identify improvement opportunities in process, procedures, infrastructure, and logging tools.

NKU specifics
Provide References
Provide Background
Sign confidentiality agreement
Expect work completion within 2 weeks and final presentation within 30 days of contract.
Sections may be awarded separately or to an individual vendor.
Scope of sections may be tailored to make best use of budgeted amount.

Award will be based on:

Ability to meet Audit Objectives
Pricing
Higher Education References
Qualifications/credentials of employees performing test
Company Background

Pricing

Should be presented for the following 4 sections:
Including

Hours of labor
Administrative cost for reporting, presentation, material, etc.

		Fee or Cost
I Internal Assessment		
Estimated Hours	_____	_____
Administrative cost		_____
Other		_____
Total Cost		_____
II Physical Security		
Estimated Hours	_____	_____
Administrative cost		_____
Other		_____
Total Cost		_____
III Wireless Assessment		
Estimated Hours	_____	_____
Administrative cost		_____
Other		_____
Total Cost		_____
IV Internet & Web Assessment		
Estimated Hours	_____	_____
Administrative cost		_____
Other		_____
Total Cost		_____
V Total Assessment		
Pricing with discounts noted for successfully obtaining all 3 sections.		
Estimated Hours	_____	_____
Administrative cost		_____
Other		_____
Discounts		_____
Total Cost		_____

General RFP Background

A. Addenda/Clarifications

Any University changes to this RFP will be made by written addendum. Verbal modifications will not be binding. Questions or comments regarding this RFP must be in writing and must be received by Eli Baird no later than **2:00 PM EDT, Wednesday, July 19, 2012** (see page 2 for contact information). Inquiries will not be accepted after the above listed date and time.

B. Confidentiality

In accordance with KRS 45A.085 Competitive Negotiation, all proposals received or information derived therefrom remain confidential until a contract is awarded or all proposals are rejected. **2012 NKU IT SECURITY & NETWORK AUDIT– NS -49-12 NORTHERN KENTUCKY UNIVERSITY**

C. Proposal Evaluation Process

All proposals received will be reviewed by the University Procurement Services office for completeness of items requested in this RFP. All complete proposal responses will be afforded equal consideration by the members of the Selection Committee. Post-bid interviews with pre-determined questions will be conducted on the top 3 (three) proposals. From these 3 (three) proposals a winner will be determined by the following process:

1. All complete proposals will be evaluated using a numerical rating system designed to afford each selection committee member a reasonable, individual, objective standard to equate the qualifications of the respondents.
2. Each selection committee member will review, consider, evaluate and assign a numerical score to each proposal. All proposals will be graded, and the three highest numerical scores will be ranked in order with the respondent having the highest score in first place, the second highest score in second place, followed by the third highest score.
3. Each committee member shall then indicate, in writing, their choices for first, second and third place, with total scores determining the bid choice.

D. Pre-Contractual Expenses

Pre-contractual expenses are defined as expenses incurred by the respondent in:

1. preparing its proposal in response to this RFP;
2. submitting its qualifications to the University;
3. negotiating with the University any matter related to this submittal; or,
4. any other expenses incurred by a respondent prior to the date of award of a contract to the selected respondent.

The University shall not, in any event, be liable for any pre-contractual expenses incurred by the respondents in the preparation of their submittals.

E. Contract Award

Issuance of this RFP, receipt of proposals, and completion of the selection process does not commit the university to award a contract. The University reserves the right to postpone opening for its own convenience, to accept or reject any or all proposals received in response to their RFP; to negotiate with other than the selected respondent should negotiations

with the selected firm be unsuccessful or terminated; to negotiate with more than one respondent simultaneously; to cancel all or part of the RFP; and to waive technicalities.

F. Electronic Responses

Electronic responses are not permitted.

G. Personal Services Contract

This RFP is for consulting or other personal services. Kentucky law requires a Personal Services Contract to be signed by the vendor and filed with the Legislative Research Commission in Frankfort prior to any work beginning. KRS 45A.690 defines a Personal Service Contract as "an agreement whereby an individual, firm, partnership, or corporation is to perform certain services requiring professional skill or professional judgment for a specified period of time at a price agreed upon."
After Determination but prior to award, a Personal Services Contract will be sent to the winning offer or for signature. Please be sure to sign and return the original contract promptly to Northern Kentucky University. A Notice of Award will not be issued until the signed Personal Services Contract has been received by Procurement Services and filed with the Legislative Research Commission in Frankfort, KY.

Regarding Personal Service Contract Invoicing

House Bill 387 has now amended Kentucky Revised Statute 45A.695(10)(A) with the following language, "No payment shall be made on any personal service contract unless the individual, firm, partnership, or corporation awarded the personal service contract submits its invoice for payment on a form established by the committee". The Personal Service Contract Invoice Form shall be used for this purpose and for you convenience we have added fields so that it can be filled in online and printed. This form can be located on Northern Kentucky University's Procurement Services website at: http://procurement.nku.edu/departmental_forms/PSC_INVOICE_FORM.pdf

H. Foreign Corporations

A. Foreign Corporations are defined as corporations that are organized under laws other than the laws of the Commonwealth of Kentucky. Foreign Corporations doing business within the Commonwealth of Kentucky are required to be registered with the Secretary of State, New Capitol Building, Frankfort, Kentucky and must be in good standing. **NKU FINE ARTS AND LIBRARY ROOF REPLACEMENT REQUEST FOR PROPOSAL TO PROVIDE PROFESSIONAL SERVICES RFP – NS -37-12 NORTHERN KENTUCKY UNIVERSITY 11**

B. The Foreign Corporate Proposer, if not registered with the Secretary of State at the time of the Bid submittal, shall be required to become registered and be declared in good standing prior to the issuance or receipt of a contract.

C. Domestic Corporations. Domestic corporations are required to be in good standing with the requirements and provisions of the Office of the Secretary of State.

I. Occupational License
Northern Kentucky University was annexed by the City of Highland Heights in 2008. All contractors performing work for NKU must possess a Campbell County Occupational License and a City of Highland Heights Occupational License (administered by Campbell County) and must also pay applicable payroll taxes. For further information call 859.292.3884 or log onto: http://www.campbellcountyky.org/home/services/occupational-license.htm.

J. Northern Kentucky University - Overview

Northern Kentucky University, located in the Greater Cincinnati metropolitan area about 7 miles south of downtown Cincinnati, was founded in 1968. The first building on the new campus in Highland Heights opened in August 1972. The campus sits on rolling land near the intersection of I-275 and I-471. Due to topography, many locations on campus have attractive views, including views of the Cincinnati skyline.

The university has sustained consistent growth through the years; unfortunately, physical resources have not kept pace with enrollment growth. Based upon 2009 data, NKU has 71 E&G ASF per FTE; similar Kentucky public institutions have an average of 137 E&G ASF per FTE (this average includes NKU). While primarily a commuter campus, NKU has 1,850 residence hall beds.

NKU owns about 425 acres and has 3.3 million GSF.

Today, with enrollment of nearly 15,748 students, Northern is now the second largest university in the Greater Cincinnati area.

For general information about NKU, visit: http://admissions.nku.edu/why/index.php

The university's master plan can be downloaded, Executive Overview:
http://campusplan.nku.edu/docs/NKU_Executive_Summary__Complete_102010.pdf

or, the full report: http://campusplan.nku.edu/docs/NKU_REPORT_Complete_102010.pdf

AUTHENTICATION OF BID, STATEMENT OF NON-COLLUSION, NON-CONFLICT OF INTEREST AND BIDDER CERTIFICATIONS

By signing below the Contractor swears or affirms, under the penalty of false swearing as provided by KRS 523.040, that he/she is in compliance with all of the following:

1. That I am the bidder (if the bidder is an individual), a partner in the bidder (if the bidder is a partnership), or an officer or employee of the bidding corporation having authority to sign on its behalf (if the bidder is a corporation).

2. That the submitted bid or bids covering the Bid Package indicated have been arrived at by the bidder independently and have been submitted without collusion with, and without any agreement, understanding or planned common course of action with any other contractor, vendor of materials, supplies, equipment or services described in the Invitation for Bid, designed to limit independent bidding or competition; as prohibited by provision KRS 45A.325;

2A. Any agreement or collusion among bidders or prospective bidders which restrains, tends to restrain, or is reasonably calculated to restrain competition by agreement to bid at a fixed price, or to refrain from bidding, or otherwise, is prohibited. The provisions of KRS 365.080 and 365.090, which permit the regulation of resale price by contract, do not apply to sales to the State.

2B. Any person who violates any provisions of Kentucky Revised Statute 45A.325 shall be guilty of a felony and shall be punished by a fine not less than five thousand dollars nor more than ten thousand dollars, or be imprisoned not less than one year nor more than five years, or both such fine and imprisonment. Any firm, corporation, or association which violates any of the provisions of KRS 45A.325 shall, upon conviction, be fined not less than ten thousand dollars nor more than twenty thousand dollars.

3. That the content of the bid or bids have not been communicated by the bidder or its employees or agents to any person not an employee or agent of the bidder or its surety on any bond furnished with the bid or bids and will not be communicated to any such person prior to the official opening of the bid or bids;

4. That the bidder is legally entitled to enter into the contracts with the Commonwealth of Kentucky and is not in violation of any prohibited conflict of interest, including those prohibited by the provisions of KRS 45A.330 to .340 and 164.390; and

5. That I have fully informed myself regarding the accuracy of the statements made, including Bid Amount.

6. Unless otherwise exempted by KRS 45.590, the Bidder intends to comply in full with all requirements of the Kentucky Civil Rights Act and to submit data required by the Kentucky Equal Employment Act upon being designated the successful bidder.

7. That the Bidder, if awarded a contract, would not be in violation of Executive Branch Code of Ethics established by KRS 11A.990.

8. Campaign Finance Laws Pursuant to KRS 45A.110 and KRS 45A.115 the undersigned hereby swears or affirms, under penalty prescribed by law for perjury, that neither he/she, individually, nor, to the best of his/her knowledge and belief, the corporation, partnership, or other business entity which he/she represents in connection with this procurement, has knowingly violated any provisions of the campaign finance laws of the Commonwealth of Kentucky, and that the award of a contract to him/her, individually, or the corporation, partnership or other business entity which he/she represents, will not violate any campaign finance laws of the Commonwealth.

9. Worker's Compensation and Unemployment Insurance Pursuant to KRS 45A.480, the undersigned hereby swears or affirms, under penalty of perjury, that all contractors and subcontractors employed, or that will be employed under the provisions of this contract shall be in compliance with the requirements for worker's compensation insurance under KRS Chapter 342 and unemployment insurance under established KRS Chapter 341.

10. Vendor Report of Prior Violations The Bidder/Owner shall reveal to the University, prior to this award of a contract, any final determination of a violation by the Contractor within the previous five (5) year period of the provisions of KRS Chapters 136, 139, 141, 337, 338, 341, and 342. The Contractor is further notified this statute requires that for the duration of this contract, the Contractor shall be in continuous compliance and the Contractor's failure to reveal a final determination of a violation or failure to comply with the cited statutes for the duration of the contract, shall be grounds for the Contractor's disqualification by the University from eligibility to bid or submit proposals to the University for a period of two (2) years. Please list any final determination(s) of violation(s) including the date of determination and the state agency issuing the determination. If no violations have occurred, type **none** in the space below.

* KRS Chapter 136 - Corporation and Utility Taxes; * KRS Chapter 139 - Sales & Use Tax; * KRS Chapter 141 - Income Taxes; * KRS Chapter 337 - Wages & Hours; * KRS Chapter 338 - Occupational Safety & Health of Employees; * KRS Chapter 341 –

Unemployment Compensation; * KRS Chapter 342 - Worker's Compensation

KRS VIOLATION	DATE	STATE AGENCY
_____	_____	_____
_____	_____	_____

READ CAREFULLY - SIGN IN SPACE BELOW - FAILURE TO SIGN INVALIDATES BID or OFFER

AUTHORIZED SIGNATURE: _____
DATE: _____
NAME (Please Print Legibly):
_____

FIRM: _____
FED ID.#:_____

PERMANENT ADDRESS:
_____
STREET CITY STATE ZIP

CONTACT PERSON: _____

TITLE: _____

TELEPHONE NO: _____ FAX NO: _____
E-MAIL: _____
****

State of _____)

County of _____)
The foregoing statement was sworn to me this _____ day of_____, 20 _____, by _____.
_____
(Notary Public)
My Commission expires: _____

THIS DOCUMENT MUST BE NOTORIZED