Burnsville · Eagan · Savage

Regular Meeting Agenda

Diamondhead Education Center
200 W. Burnsville Parkway
Burnsville, MN 55337
June 6, 2017
4:45 PM

I. Welcome/Intro
II. Internet / ISP Consultation Review 2
III. Next Month Meeting Agenda
IV. Adjourn

District 191 welcomes members of the public to attend Board of Education meetings, work sessions and other public gatherings. However, public participation is allowed only during listening sessions, which are held before regular board meetings. Community members who wish to share their thoughts and opinions on meeting topics should contact the Superintendent's office at 952-707-2005 to schedule a meeting with the Superintendent or member of her leadership team.

Burnsville Public Schools

Network, Systems, and Security Audit

SOW #T20170418.0148

5/2/17

Table of Contents

About

Burnsville-Eagan-Savage School District 191 serves approximately 9,000 students across 10 elementary schools, three middle schools, and two high schools. Burnsville Public Schools has attracted the attention of Best Buy and Google for their innovation. Recently they experienced a network outage that affected the entire district. That event has led to Burnsville Public Schools desiring a third-party audit of their network, systems, and security.

Project Overview

Third-Party Audit

Burnsville Public Schools has requested an external audit of Systems, Networks, and Security of their environment. We will provide that audit covering the areas of: physical security; external scans of environment; Chromebook and iPad security review; network review including layer 3, layer 2, firewalls; system review including virtualization, storage, Active Directory, general systems review, database review.

As audits can be wide and/or deep, Atomic Data is providing the list of items we would recommend doing and the deliverables for those items. Burnsville Public Schools can redline specific areas that are not areas that deep diving is needed or required.

Estimated Project Schedule

Start Date	Once Signed	Completion Date	45-60 Days

Assumptions

1. Atomic Data assumes that we will be given a Domain Administrator account to use with our data collection agents.
2. Atomic Data assumes we can load an agent on all Windows Servers in the environment.
3. Atomic Data assumes we will be given access to the virtualization environment.
4. Atomic Data assumes we will be given access to the storage environment.
5. Atomic Data assumes that we will be granted read-only access on all networking equipment.
6. Atomic Data assumes that we will be given time to interview core resources for the security review.

7. Atomic Data assumes our external scanning will not impact Burnsville Public Schools externally facing services.

Scope of Work

The following services will be provided on a time and materials basis:

IT Managed Services

1. Provide a 3rd Party Audit of ISD191's network, systems, and security.

Project Deliverables

Deliverables may be improved or modified by the direction of the client throughout the process of implementation through a Change Order. Below is the initial list of deliverables:

1 Site Visits and Physical Inspections

Atomic Data will send an engineer to each site to physically inspect location for security, cabling, and equipment. We will provide as a deliverable a full inventory report of all networking equipment.

Deliverable: Inventory Report of all physical equipment (network gear, servers, storage systems). This will be included in a high-level Operations Report.

Specifications: Labor

2 External Vulnerability Scans and Reports

Atomic Data will perform an external vulnerability scan of Burnsville Public Schools Internet-routable IP ranges.

Deliverable: Summary and detailed reports highlighting vulnerabilities identified during the external vulnerability scan. Summary report will provide a broad overview of the security of the school's perimeter, while the detailed report (provided as a spreadsheet) will include detailed information about each Internet-accessible host and any identified vulnerabilities. This will be included in a high-level Security Report.

Specifications: Labor

3 Chromebook and iPad Security Review

Atomic Data will review sample Chromebook and iPads in use by students and determine security risks and vulnerabilities exposed to students and to the district's environment. Review will be performed against current best-practices and any benchmarks published by CIS or NIST.

Deliverable: This subject will be discussed in a high-level Security Report.

Specifications: Labor

4 Layer 3 Network Review

Atomic Data will review the layer 3 portions of the network. We will produce layer 3 diagrams showing how data moves around the environment.

Deliverable: Layer 3 Network Diagrams. This subject will be discussed in a high-level Operations Report.

Specifications: Labor

5 Layer 2 Network Review

Atomic Data will review the layer 2 portions of the network. We will produce layer 2 diagrams showing how data moves around the environment.

Deliverable: Layer 2 Network Diagrams. This subject will be discussed in a high-level Operations Report.

Specifications: Labor

6 Firewall Review

Atomic Data will review the firewall configurations in place. We will produce information for how data ingresses and egresses the network.

Deliverable: This subject will be discussed in a high-level Security Report.

Specifications: Labor

7 Virtualization Review

Atomic Data will review the virtualization environment. We will review configurations, best practices, and document all hypervisors and guests.

Deliverable: Inventory Report of all hypervisors and guests. This subject will be discussed in a high-level Operations Report.

Specifications: Labor

8 Storage Review

Atomic Data will review the storage environment. We will review configurations, best practices, and document all storage arrays.

Deliverable: Inventory Report of all storage systems. This subject will be discussed in a high-level Operations Report.

Specifications: Labor

9 Active Directory Review

Atomic Data will review the Active Directory environment for configuration, password policies, and best practices.

Deliverable: Detailed Report of Active Directory configuration including security components. This subject will be discussed in a high-level Operations Report.

Specifications: Labor

10 Systems Review

Atomic Data will inventory all virtual servers and physical servers. We will dig into areas of concern and provide list of recommended changes.

Deliverable: Detailed Report of all servers including installed applications. This subject will be discussed in a high-level Operations Report.

Specifications: Labor

11 Database Review

Atomic Data will review database servers for configurations, performance, backups, security, and other areas of concern.

Deliverable: This subject will be discussed in a high-level Operations Report.

Specifications: Labor

12 Security Interviews - Discovery and Report

Atomic Data will interview multiple individuals to construct a security profile of operational tasks within the Burnsville Public School District. Interviews will include the following topics:

- Identity and Access Management
- Change Management
- Security Policies / Procedures
- Risk Management Practices
- Implemented Security Controls and Technologies
- Security Incident Management
- Security Management Practices

Security interviews are intended to help establish the organization's overall security posture and help identify program-level opportunities for improvement.

Deliverable: This subject will be discussed in a high-level Security Report.

Specifications: Labor

Estimates

The estimated effort for the Statement of Work is detailed below.

Deliverables	Min Effort	Max Effort
1 Site Visits and Physical Inspection	100	120
2 External Scans and Reports	10	12
3 Chromebook and iPad Security Review	8	12
4 Layer 3 Network Review	12	20
5 Layer 2 Network Review	30	40

6 Firewall Review	20	30
7 Virtualization Review	18	20
8 Storage Review	8	10
9 Active Directory Review	4	5
10 Systems Review	25	30
11 Database Review	12	15
12 Security Interviews – Discovery and Report	32	36
Total Estimated Effort	**279**	**350**

Please note – these estimates are not a fixed bid. Additional requests and modifications to the scope of work may require a change order and will be handled outside this statement of work.

Project Management

Atomic Data provides both technical expertise and project management expertise. Our Senior Architects and Project Managers have several years of enterprise configuration and implementation experience that will help keep the team on task and the overall project on schedule and within budget. A primary key to successful configuration and implementation projects are frequent but brief status updates with every team member. Atomic Data employs the concept of internal Recurring Status Meetings to keep the team on track and to identify schedule slippage or issues as they occur, not after it's too late to make an adjustment.

Next Steps

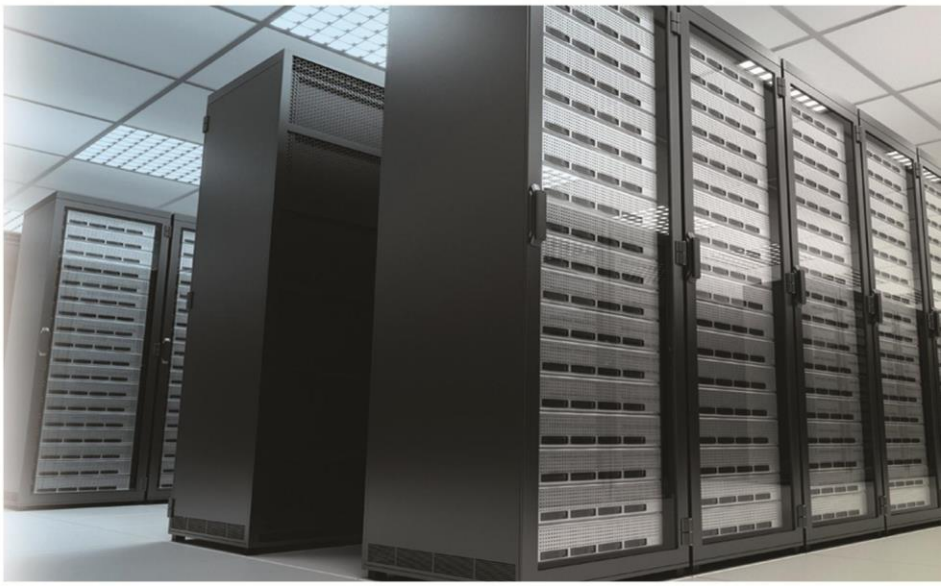
Once this document is acknowledged and accepted, the next step is to review the quotes that accompany this document. The signing of the quotes will initiate the implementation of the work outlined in this scope of work.

ACKNOWLEDGED AND ACCEPTED:

Burnsville Public Schools	ATOMIC DATA
Name	Name

Date	Date
Signature	Signature

HEARTLAND BUSINESS SYSTEMS



Minnesota Independent School District #191

Statement of Work

Security Assessment

Presented by

Heartland Business Systems

April 27, 2017

APPLETON, WI
MILWAUKEE, WI
MADISON, WI
EAU CLAIRE, WI
CHICAGO, IL
BLOOMINGTON, MN
DES MOINES, IA

Contact Information

Minnesota Independent School District #191

Doug Johnson

100 River Ridge Court
Burnsville, Minnesota 55337
952-707-2065
dajohnson@isd191.org

Heartland Business Systems

Josh Streich
Sales Consultant
920-687-4135
jstreich@hbs.net

Andrew Hull
Information Security Officer
920-687-4109
ahull@hbs.net

Document Revision History

Date	Version	Change made	Changed by
April 27, 2017	1	Initial Statement of Work	Andrew Hull

Table of Contents

Initiation

Heartland Business Systems (HBS) engineers will work with Minnesota Independent School District #191 to identify, define, unify, and coordinate strategy and implementation efforts from project inception to project close. We want this project to be a success for you; both short term and long term. Our team and process work together to complete the project on time, within budget, and within scope**.**

Purpose of Document

This Statement of Work (SOW) describes the professional services to be provided by Heartland for Minnesota ISD #191. It describes the deliverables, schedule, as well as the approval and change control process. When mutually executed for implementation, this SoW becomes contractually binding on HBS and Minnesota ISD #191 under the terms and conditions of the HBS Standard Terms and Conditions (STC) document.

Executive Project Overview

Heartland Business Systems is pleased to present the attached proposal to assist Minnesota Independent School District #191 (Minnesota ISD #191) in its' evaluation of its network security. HBS has created this customized statement of work, based on its core offerings, that will encompasses the following key areas of analysis and testing. These areas include:

- External Vulnerability Assessment
- Internal Vulnerability Assessment
- Wireless Security Assessment
- Social Engineering Assessment (phone, email, physical)
- Cyber Security Framework Controls Assessment
- IT Contingency Assessment

It is important to note that security testing will not include exploitation attempts on systems that have been found to have vulnerabilities, as exhaustive penetration testing can often create instabilities in systems and applications. It is the intent to only report on discovered vulnerabilities and provide recommendations for remediation.

At the end of the engagement, Heartland Business Systems will deliver a professional report that includes an executive summary, technical summary, as well as the technical details of our findings and remediation recommendations. Any critical issues identified while performing the assessment will be reported expediently after validation, and prior to the final report.

Order of Precedence

Any ambiguity or inconsistency between or among the terms of this SoW and the STC shall be resolved by giving priority and precedence in the following order:

1. This Statement of Work (SoW)
2. Standard Terms and Conditions (STC)
3. Non-Disclosure Agreement (NDA), if not incorporated in the STC

Anything not addressed in this SoW is out-of-scope and not included in these quoted services. Either party may submit a Change Request to the other party, in accordance with the HBS Change Request process identified in Appendix A of this document, to modify the scope of this project.

Scope

Heartland Business Systems works to ensure that projects include the work required to successfully complete the project or statement of work. In scope and out of scope items are detailed to confirm all project components and work being completed.

In Scope

The following areas are considered in-scope for this SoW:

- ***External Vulnerability Assessment***

  The external testing is designed to help Minnesota ISD #191 understand its current exposure related to providing externally available, internet based, IT services. In order to identify possible system weaknesses, Heartland will leverage a range of network information gathering and testing techniques including vulnerability scanning and analysis. These actions will be conducted from an unauthenticated perspective using tools and techniques similar to what a hacker would utilize when performing reconnaissance on potential targets. Heartland Business System utilizes a wide range of tools to perform these actions, from publically available to world-class commercial testing tools. In execution of this aspect of the scope, HBS will:

  - Perform targeted security testing of all IP addresses, in the specific IP address ranges provided below by the customer, to determine if technical vulnerabilities exist.

IP Address Range(s)	Total IP's	Active IP's not to Exceed
204.169.30.0/24 204.169.32.0/24 204.169.37.0/24	762	280

  - This assessment will be performed from a public Internet point of view, sourced from a Heartland owned IP space. We will use mostly safe checks covering network-based vulnerabilities, patch/hotfix/secure configuration checks, and some web application-layer testing. These tests are designed to not likely be disruptive to Minnesota ISD #191. Heartland will not perform any Denial of Service (DoS) testing on targeted hosts. In execution of this assessment, we will;
    - Review external security through network reconnaissance and other information gathering techniques.
    - Perform targeted vulnerability testing of the in-scope IP addresses looking for known vulnerabilities.
    - Analyze reports and data generated by testing software to assess risks.
    - Develop customized remediation recommendations based on the severity of findings and the environment.
    - Prioritize remediation recommendations according to risk
  - If a specific testing window is to be adhered to, this timeframe must be provided to HBS within three (3) business days of execution of this SoW.
  - Virtual meeting for the delivery of a comprehensive vulnerability report containing an executive summary, itemization of vulnerabilities and their severities, as well as recommended remediation options for each vulnerability identified.

- ***Internal Vulnerability Assessment***

  The internal vulnerability assessment will be used to help Minnesota ISD #191 identify internal security vulnerabilities on its current deployment of internal network and server equipment as well as its standard client access devices, such as computers and printers. Heartland will perform authenticated tests using privileged credentials provided by Minnesota ISD #191 as well as specialty tools. The goal is to determine whether internal systems can be exploited by an attacker or used to gain access to sensitive information. In execution of this aspect of the scope, HBS will:

  - Perform targeted security testing of all IP addresses, in the specific IP address ranges provided below by the customer, to determine if technical vulnerabilities exist.

IP Address Range(s)	Active IP's not to Exceed
All Infrastructure (Servers & Network Equipment) RFC1918 Addresses in 18 Locations	1,000
Sample of Managed Client Access Devices (iPad/Chromebook/Windows) RFC1918 Addresses TBD in 18 Locations	3,300

    - While Heartland recognizes it only takes one vulnerable device to facilitate a security issue, a 30% random sampling approach is believed to be a fiscally responsible and valid measurement of internal vulnerabilities on client access devices. This is due to both the tools and techniques the customer has deployed to centrally manage these devices, as well as the fact that Minnesota ISD #191 has never performed this type of assessment. Heartland recommends future internal assessments should include all internal assets.
  - This will be done from an internal and authenticated point of view, with authorized credentials provided by the Customer. We will only use safe checks, including network-based vulnerability, patch/hotfix/security configuration checking, and some application-layer testing. This assessment will not "attack" the infrastructure or perform any DoS actions on targeted hosts. In execution of this we will:
    - Perform targeted vulnerability testing of the in-scope IP addresses to determine known vulnerabilities exist
    - Analyze reports and data generated by testing software to assess risks.
    - Develop customized remediation recommendations based on findings and the customer environment
    - Prioritize remediation recommendations according to risk
  - HBS will come on-site and connect HBS devices to the customers' internal network.
  - HBS and Customer work together to install a remote testing environment on customers' internal network.
  - If a specific testing window is to be adhered to, this timeframe must be provided to HBS within three (3) business days of execution of this SoW.
  - Virtual meeting for the delivery of a comprehensive vulnerability report containing an executive summary, itemization of vulnerabilities and their severities, as well as recommended remediation options for each vulnerability identified.
  - Customer responsibilities;
    - Customer to supply Heartland two (3) Internal IP's (including IP, subnet mask, default route, and DNS IP's) to preconfigure the onsite equipment

- Provide client based full VPN connectivity to HBS security resources for remote management of the installed equipment on customers' site.
- Allow the on-site security consultants' devices un-authenticated outbound Internet connectivity
- Allow the installed devices unrestricted internal IP access.
- Provide at least 20Mbps of available Internet and WAN connectivity during testing timeframes.

- ***Wireless Security Assessment***

  Since wireless LAN technology is used by a significant number of access devices, many of which have access to sensitive information, HBS will be conducting a review of all Wireless LAN device configurations. This assessment will tell Minnesota ISD #191 if configuration concerns exist that could lead to someone gaining unauthorized access to network resources via the wireless network. In execution of this aspect of the scope, HBS will:

  - Perform a best practices configuration and security assessment of Minnesota ISD #191's two (2) Wireless LAN Controller (WLCs) configurations for two different Access Point models. This work will be conducted remotely and will include the following components:
    - Heartland will perform discovery on the WLC's.

Access Point Models	Number of Controllers	Quantity of Unique SSID's
Extreme Altitude 4620	1	Up to 4
Aruba IAP-225	1	Up to 4

    - Heartland will assess WLC configurations, identify and document areas of concern
    - Heartland will make recommendations based on "best practice" configurations, field experience, and knowledge of Company's future expansion needs.
    - Heartland Engineer will document its recommendations and give instructions on how to make any necessary configuration changes.

- ***Social Engineering Assessment***

  Social engineering is one the most commonly used tactic across all levels of adversaries to gain unauthorized access to networks and information. Hackers manipulate people into performing actions or divulging confidential information by masquerading as an authorized person. They attempt to trick an employee or contractor into divulging information or permitting access in order to bypass security measures and tools. This technique is often easier than using technical hacking or physical break-in techniques. While many organizations attempt to implement policies and controls to mitigate this threat, unauthorized access through social engineering attacks are usually highly successful. A proven way to assess an organization's risk related to these threats is to test the effectiveness of existing controls and policies. Social engineering assessments are designed to help our customers effectively evaluate their organizations risk of social engineering attacks. Heartland utilizes proven processes and technologies to evaluate weaknesses in customers' identification and response activities to help measure the risk of unauthorized access to critical information and systems. Social engineering assessments identify gaps where targeted security training may be needed to be developed or enhanced. In execution of this aspect of the scope, HBS will:

- Perform an Email Phishing campaign against the Minnesota ISD #191s' staff using an agreed upon real world scenario, in conjunction with our methodical and standardized approach. The objective of the assessment is to identify areas of weakness in employee's adherence to email security best practices.
    - Testing will be designed to entice up to 500 random employees to visit an unknown website or to open a malicious email attachment.
    - Heartland will document the summary results of their assessment and provide recommendations for helping to prevent or reduce the impact of these types of attacks.
- Perform a phone based pretexting social engineer campaign against the customers' staff using real world scenarios, in conjunction with our methodical and standardized approach. The objective of the assessment is to identify areas of weakness in employee's adherence to security best practice.
    - Testing will be designed to entice up to 30 employees to visit an unknown website (site created as part of the email phishing scope) or to provide protected information.
    - Heartland will document the summary results of their assessment and provide recommendations for helping to prevent or reduce the impact of these types of attacks.
- Perform covert physical access assessment at three (3) physical locations, whereby an HBS employee will attempt to gain undetected and unauthorized access to:
    - Internal network resources
    - Data center or data closets
- Customer Responsibilities;
    - Provide Heartland valid email addresses for employee targets
    - Ensure targeted emails, links, or attachments are not blocked by the company's technical security controls
    - Provide Heartland up to 30 employee names and phone numbers to be targeted
    - Ensure targeted emails, links, or attachments are not blocked by the company's technical security controls
    - Provide Heartland physical address information for up to 3 locations to be targeted for physical access

- ***Security Architecture and Best Practices Review***

  The NIST Cyber Security Framework (CSF) will be used as the framework for the security architecture and best practices assessment. Using standards based frameworks helps to ensure a balanced approach to security as well as ensure your security and privacy controls do not have any blind spots. The National Institute of Standards and Technology (NIST) has published this guidance to enable organizations, regardless of size, degree of cyber security risk, or cybersecurity sophistication, to apply principles and best practices for the purposes of improving the security and resilience of their infrastructure. This framework provides organization and structure to today's multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively in most every industry today. In execution of this aspect of the scope, HBS will:

  - Perform a security architecture review of Minnesota ISD #191's with focus on technical, physical, and administrative controls used to protect student and faculty technology, as well as data collected by Minnesota ISD #191. The review will be based on today's most common

threat vectors facing K-12 environments. Focus will be on measuring Minnesota ISD #191's ability to protect, identify, detect, respond, and recover from security related incidents. This work will be conducted both remotely and onsite and will include the following components:

- Review of technical security architecture through;
  - Network diagram reviews
  - Technical resource interviews
- Review of Minnesota ISD #191's technical, physical, and administrative controls through interviews
- Review how confidential information is protected
- Review security incident detection and response
- Review IT Contingency mechanisms and practices
- Report of Findings and Recommendations regarding Minnesota ISD #191's Cyber Security Preparedness
- Virtual meeting with key personnel for the purposes of discussing Heartlands finding report and recommendations

- ***IT Contingency Assessment***

The IT Contingency Assessment will be used to assess Minnesota ISD #191s' existing business continuity as well as disaster recovery plans necessary to help ensure the survivability of Heartland Business Systems's business, if a business interruption event were to occur. This will include review of the necessary structure and supporting documentation needed to ensure business expectations are being met, best practices are being consistently followed, ensure the plans are properly maintained and tested over time. In execution of this aspect of the scope, HBS will:

- Conduct Business Impact Analysis:

  - Review and document business resumption related threats used for contingency planning
  - Review technology dependencies with business deliverables

- Perform IT Asset Inventory and Criticality Mapping:

  - Define what IT assets support which business applications
  - Conduct a business application review
  - Review customer provided system inventory of IT assets
  - Provide report of discovered assets mapped to a criticality rating

- Contingency Plan Review:

  Review formal written documentation for response practices, recovery strategies, and tactical procedures to respond to a variety of scenarios (power outages, inaccessibility to building(s), facilities loss, single system failure, etc.).

  - Review the following critical plan components;
    - Team Roles
    - Disaster Recovery Declaration Procedure
    - Business Contact Information

        - Business Owner
        - Upstream and Down Stream Business Owners
    - Primary / Secondary IT Support Contacts
    - Vendor / Supplier Contact Information
    - Licensing Information
    - Detailed Physical Location (Address, Room number, etc.)
    - Existing configuration and change management procedures
    - Existing System Shutdown and Startup Procedures
    - Existing System and Application Recovery Procedures
    - Existing application flow diagrams
    - Existing infrastructure diagrams

- Review previously performed contingency tests to ensure that Minnesota ISD #191 maintains and stays current with the business and recovery objectives it is important to regularly evaluate and test the plan and update it when changes occur in the environment.
- Document a Recovery Risk Assessment:
    - Assess the technical and procedural controls in place to identify vulnerabilities so that management has the information necessary to make decisions on how to manage risk.
    - Conduct interviews with Minnesota ISD #191's IT team to understand current strategies for recovery of IT services
    - Document gaps in current strategies that would not meet recovery objectives

Out of Scope

The following areas are considered out-of-scope for this SoW:

- Assessment of customer's compliance with any industry, state or federal regulations or guidance
- Security Incident response of any kind
- Computer forensic services of any kind
- Remediation of any vulnerabilities identified
- Anything not specifically called out as "In Scope" above

Key Assumptions

Minnesota ISD #191:

- Will make appropriate personnel available for meetings and interviews as required.
- Will make all appropriate and requested documentation available in a timely fashion
- Will assign an IT representative for the duration of the test to be available for status updates and an emergency contact in case of perceived testing related issues
- Will agree to all provisions in the security testing permission agreement before testing is initiated
- Will provide Heartland internal network access, including all necessary connectivity and credentials, to perform the internal vulnerability testing
- Will "whitelist" Heartland provided source IP's in customers Intrusion Prevention System

- Will provide Heartland the specific network IP's or IP ranges, for which customer is authorized, that are to be in scope of the testing
- Will provide Heartland with a listing of IP addresses that are out-of-bounds
- Will provide Heartland with any timeframes that testing should not occur (these will be considered blackout periods).
- Will provide VPN remote access so Heartland can manage the remote testing equipment
- Will provide the appropriate environmental and facilities for HBS equipment and personnel in the testing location(s)
- Will provide DNS resolution for internal and external name spaces
- Will provide credentials to log into the Wireless LAN Controllers
- Will provide names, email address and telephone numbers for social engineering
- Will provide physical location addresses for sites to be included in physical social engineering

Heartland Business Systems:

- Will inform designated customer IT Representative of the timeframe(s) for testing
- Will assign a senior consultant to act as the engagement manager and be available for communication with the customer during the length of the engagement.
- Will inform the designated IT representative when the testing has begun and if any of the tests are believed to have caused any interruption in services.
- Escalate any critical findings to customer's designated IT Representative immediately upon validation
- Will conduct all testing specified in the scope
- Will provide final reports, as outlined in the scope

Change Control

All items agreed upon throughout this document are considered "in-scope". Additional items beyond the statement of work are considered "out-of-scope" and are subject to additional cost. All changes will be documented and approved using the standard change control form located in *Appendix – A*.

Permission to Perform Security Testing

Certain laws prohibit any unauthorized attempt to test or penetrate computer systems. Customer acknowledges and authorizes Heartland consultants to perform the security services described above. Furthermore, the customer acknowledges that all services provided under this statement of work constitute authorized access to customers' information systems.

While the testing that Heartland security consultants will perform mostly safe checks, including network-based vulnerability identification, patch/hotfix checking and some application layer testing, some inherent risk still applies. Customer acknowledges and agrees to the following:

- Customer certifies they have the legal right to agree to sign these terms and conditions for the IP addresses customer provided to Heartland.
- Customer authorizes Heartland to perform security testing of customer's selected network assets, as defined above.
- The various reconnaissance and network tests will likely produce alerts by network and host based intrusion detection systems.

- Large amounts of log messages may be generated resulting in excessive log file disk space consumption;
- The operational availability of the customers systems and network may be temporarily degraded during the testing.
- While rare, it is possible that computer systems and/or network devices may become unresponsive or crash as a result of testing. This will require the customer to "reset" the system.
- Customer agrees to accept any and all risks associated with these services; and accepts all responsibility for the consequences of a system failure caused by the delivery of these services.

Pricing

Statement of Work Item	Price
External Vulnerability Assessment (280 Active IP's)	**$12,150**
Internal Vulnerability Assessment (4,300 Active IP's)	**$18,400**
Wireless Security Assessment (2 AP's & Controllers)	**$8,300**
Social Engineering Assessment	**$19,750**
Phishing (500 Targets)	$8,230
Telephone Pretexting (30 Targets)	$5,070
Physical Site (3 Targets)	$6,450
Security Architecture and Best Practices Review (NIST CSF)	**$9,450**
IT Contingency Assessment	**$10,350**
Total	**$78,400**

Invoicing

Heartland will pre-bill customer for this engagement upon signature of this proposal. Applicable taxes are additional.

Scheduling

We want to work towards scheduling all necessary resources and timely completion of the project. Heartland will work with you to detail all time constraints and outline the best approach to completion based upon a mutually agreed upon schedule. Typically, Heartland likes 3-4 weeks from the signing of an engagement to schedule and begin its work, but if required, we can work with you to meet your specific timing needs.

Project Closure Criteria

The project will be considered complete, when any of the following are met:

- All of the service deliverables identified within this SOW have been completed, delivered and accepted or deemed accepted, including approved Change Request Forms;
- The fee provisions of the Work Order have been met; or
- This agreement is terminated pursuant to the provisions of the agreement.

Approval & Next Steps

Upon customer approval, Heartland will begin to schedule the work immediately and a date will be negotiated for the presentation of the deliverables outlined in this statement of work.

Acceptance of Proposal

Heartland requires the Acceptance of Proposal be signed and a copy be sent back in order to start the engagement. Any changes to this document must be submitted to Heartland for review and approval. Upon notification, Heartland will revise and resubmit the document for signature. Please scan and email back the signed SOW to: tpeterson@hbs.net and ahull@hbs.net

Statement of Work (SOW) Items	***Accept***	***Decline***
External Vulnerability Assessment (280 Active IP's)..... $12,150 *Applicable taxes are additional	☐	☐
Internal Vulnerability Assessment (4,300 Active IP's) ..... $18,400 *Applicable taxes are additional	☐	☐
Wireless Security Assessment (2 AP Models / 2 Controllers)..... $ 8,300 *Applicable taxes are additional	☐	☐
Social Engineering - Email Phishing Assessment (500) ..... $ 8,230 *Applicable taxes are additional	☐	☐
Social Engineering - Telephone Pretexting Assessment (30)..... $ 5,070 *Applicable taxes are additional	☐	☐
Social Engineering – Physical Covert Onsite Assessment (3)..... $ 6,450 *Applicable taxes are additional	☐	☐
Security Architecture and Best Practices Review ..... $ 9,450 *Applicable taxes are additional	☐	☐
IT Contingency Assessment ..... $10,350 *Applicable taxes are additional	☐	☐
Acknowledgement & Permission to Perform Security Testing ..... *Must be accepted before any vulnerability testing can begin	☐	☐

	Minnesota ISD #191	**Heartland Business Systems**
Signature:	_____	Signature: _____
Name:	_____	Name: _____
Title:	_____	Title: _____
Date:	_____	Date: _____

Appendix A: Change Control Form

Customer:	<Client>
Project Name:	
Project Number:	SVXXXXXXX

General Information

Person Submitting Change:	<PM>		
Date Submitted:	<Date>	**Submitter Phone/Email:**	
Person Requesting Change:	<Client Sponsor>		
Date Requested:	N/A	**Requester Phone/Email:**	

Proposed Change

Title of Change:	
Description of Change:	
Reason for Change:	

Project Manager Review of Change (COMPLETED BY PROJECT MANAGER)

Hardware Required for Change:	**Provided by customer**		
Software Required for Change:	**Provided by customer**		
Action Required for Change:	**Additional time needed to**		
Timeline Impact:	**hrs**	**Cost Impact:**	
Resource Impact:	**N/A**		
Quality Impact:	**N/A**		
Overall Impact:	**N/A**		
Additional Comments:	**N/A**		

Approval of all Changes (COMPLETED BY THE CUSTOMER)

Change Approved by:	
Date:	
Signature:	

District ONE 91
Future Ready. Community Strong.

Douglas A Johnson <dajohnson@isd191.org> 26

Architecture Overview, Business Impact Assessment(BIA) & Security Assessment

3 messages

Steven Smith <Steven.Smith@ties.k12.mn.us> Mon, May 1, 2017 at 6:42 PM
To: Doug Johnson <dajohnson@isd191.org>
Cc: Ryan Cloutier <Ryan.Cloutier@ties.k12.mn.us>, Corey Tramm <Corey.Tramm@ties.k12.mn.us>

Doug,

We decided a two-phase approach would provide the maximum benefit and flexibility.

After careful consideration in order to give you the most cost effective security assessment possible, we will need to perform a Business Impact Assessment and Architectural overview, this will allow us to focus on your most critical assets and keep scope under control. Given the nature of your timelines for service interruption we want to tightly coordinate the vulnerability and network testing to your most critical assets first (hence the need for the BIA and Arch overview) and then we can scan the other assets with less disruption to the network, computing resources and people. This will also add value by giving you a map of your critical infrastructure and sensitive data that we will need to properly assess vulnerabilities

Project Summary Description

Architecture Overview

- Asset Discovery
  - **Asset Discovery** – utilizing our Unified Security Management scanning ability we will discovery all assets running on your network.
- Asset Map
  - **Asset Map –** will provide a clear map on critical infrastructure

Business Impact Assessment

- BIA
  - **BIA** - a systematic process to determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster, accident or emergency.

Project Scope and Deliverables

1. Executive summary

2. Detailed assessment findings for existing assets and sensitive data and their impact on business operations.

Once the Architecture Overview/BIA is complete we can provide an overall Security Assessment, this effort[27] will utilize the output of phase one. The Security Assessment will provide the following:

Project Summary Description

Assess Security controls

- Physical controls
    - **Physical security** describes **security** measures that are designed to deny unauthorized access to facilities, equipment and resources, and to protect personnel and property from damage or harm (such as espionage, theft, or terrorist attacks).
- Administrative controls
    - **Administrative controls** (or work practice **controls**) are changes in work procedures such as written safety policies, rules, supervision, schedules, and training with the goal of reducing the duration, frequency, and severity of exposure to cyber security threats.
- Technical controls
    - **Technical controls** are security **controls** that the computer system executes. The **controls** can provide automated protection from unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data.

Project Scope and Deliverables

3. Executive summary
4. Detailed assessment findings for Physical, Administrative and Technical controls.

The goal of these two work efforts is to clearly identify your current security posture/maturity and provide a roadmap to get more mature and develop a Legally Defensible Security Posture. This work will also provide the basis to build a Business Continuity/Disaster Recovery plan that can be customized to most cost effectively protect your environment.

Typically, we quote these types of assessments as “fixed bid” project. Based on our initial discussion around your willingness to perform some of the self-assessment interview questionnaire work we are going to provide “not to exceed pricing” you see below.

Architecture Review & BIA = $250/hour not to exceed $5,000

Security Assessment = $250/hour not to exceed $10,000

If you have any questions, please let me know. If you agree with this approach just let me know and I will send over formal Statements of Work(SOW’s)

Thanks

Steve Smith | Product Manager – Technical Services

(O) 651-999-6337 (C) 612-387-7446

TIES

Technology so you can teach

1667 Snelling Ave. N., St. Paul, MN 55108

www.ties.k12.mn.us

Doug Johnson, TechDir <dajohnson@isd191.org> Tue, May 2, 2017 at 8:52 AM
To: Steven Smith <Steven.Smith@ties.k12.mn.us>
Cc: Ryan Cloutier <Ryan.Cloutier@ties.k12.mn.us>, Corey Tramm <Corey.Tramm@ties.k12.mn.us>

Thanks, Steve. Were we to accept this proposal, what kind of timeline would work? This spring, this summer, next fall?

Doug

Doug Johnson
Director of Technology
Tel. 952.707.2065
Web www.isd191.org

200 W Burnsville Pkwy
Burnsville, MN 55337

District one91
Future Ready. Community Strong.

[Quoted text hidden]

Steven Smith <Steven.Smith@ties.k12.mn.us> Tue, May 2, 2017 at 11:19 AM
To: "Doug Johnson, TechDir" <dajohnson@isd191.org>
Cc: Ryan Cloutier <Ryan.Cloutier@ties.k12.mn.us>, Corey Tramm <Corey.Tramm@ties.k12.mn.us>

Doug, I will let Ryan answer the timeline question as he will have direct interaction. Thanks

Steve Smith | Product Manager – Technical Services

(O) 651-999-6337 (C) 612-387-7446

TIES

Technology so you can teach

1667 Snelling Ave. N., St. Paul, MN 55108

www.ties.k12.mn.us

From: Doug Johnson <dajohnson@isd191.org>
Date: Tuesday, May 2, 2017 at 8:52 AM
To: Steven Smith <Steven.Smith@ties.k12.mn.us>
Cc: Ryan Cloutier <Ryan.Cloutier@ties.k12.mn.us>, Corey Tramm <Corey.Tramm@ties.k12.mn.us>
Subject: Re: Architecture Overview, Business Impact Assessment(BIA) & Security Assessment

Thanks, Steve. Were we to accept this proposal, what kind of timeline would work? This spring, this summer, next fall?

Doug

Doug Johnson
Director of Technology
Tel. 952.707.2065
Web www.isd191.org

200 W Burnsville Pkwy
Burnsville, MN 55337

District one91
Future Ready. Community Strong.

[Quoted text hidden]