December 12, 2016

Richard Flanagan

Chairman of the Board of Directors

A+ Corporation

810 23rd Street

Philadelphia, PA 19122

Dear Mr. Flanagan,

We are pleased to respond to the Request for Proposal (RFP) dated November 30, 2016 wherein A+ Corporation (hereinafter “A+” or “Company”) is requesting bids for the performance of a specialized information security audit and associated consulting services. As a global leader in Information Technology governance, risk and compliance consulting, CRS InfoSec Solutions (hereinafter “CRS”) has provided IT audit services to a wide range of industries for more than 15 years.

The RFP states the A+ Board of Directors and Executive Management seek assurance that the newly implemented IT Data Destruction Policy (hereinafter “Policy”) is sufficiently robust; that appropriate mechanisms have been implemented to enforce and monitor adherence to the Policy; and that employees, contractors and other third parties are in fact complying with the Policy.

CRS has performed similar audits for businesses like A+ who seek to protect their information assets from cradle to grave, and to prevent data breaches and unauthorized disclosure resulting from improper disposal of data storage devices. As a result, we have identified the following generic risks associated with the destruction of computing assets that were once used to process and store personal, confidential and classified information and data:

1. The wrong hardware is identified for destruction
2. IT fails to adequately wipe the hardware
3. The wrong hardware is transferred to the destruction vendor
4. The hardware is lost in transit
5. The destruction vendor fails to destroy the hardware

The following list includes several preventive and detective controls other companies have implemented to support effective destruction of their decommissioned IT hard drives, RAM and external storage devices:

| **Control Types** | **Why They Are Important** | **Evidence That Shows Effectiveness** |
| --- | --- | --- |
| Preventive Controls |
| Asset Inventory Management Tool (AIM) | Maintains records of physical IT assets | * Results of prior independent audits
* Effective role based access controls
* Full and false inclusion testing
 |
| Asset Tagging | Unique identifiers used to support IT asset tracking | * Compare a sample of physical IT asset barcodes against AIM **{a}**
* Compare a sample of barcodes from AIM against physical IT assets **{a}**
* Investigate discrepancies
 |
| Help Desk Ticketing Tool (HDT) | Monitors the stages of IT asset decommissioning/destruction | * Examine HDT audit trails for a sample of laptops classified as “retired” in AIM
* Ascertain HDT classifies a sample of devices pending destruction as “decommissioned”
* Confirm help desk tickets were closed for a sample of destroyed equipment per select Certificates of Destruction **{b}**
 |
| Service Level Agreement (SLA) | Defines agreed upon timing, destruction methods, mutual responsibilities and sanctions; stipulates minimum security standards | * Results of prior independent audits
* Ensure SLA defines mutual responsibilities of the parties
* Verify inclusion of agreed upon destruction methods
* Assess sufficiency of sanctions for non-compliance
 |
| On-site Destruction | Prevents decommissioned IT assets from being lost/stolen during transfer to the data destruction vendor site | * Ensure provision for on-site destruction has been incorporated into the SLA
 |
| Detective Controls |
| Physical Inventories | Verifies existence; thereby validating that the right IT assets were destroyed | * Results of prior independent audits and oversight
* Refer to **{a}** above
 |
| Independent Sampling | IT management ensures data storage devices are properly wiped prior to transfer to the hardware destruction vendor | * Review results of tests performed by client to ensure proper wiping
* Reperform tests performed by client to ensure consistent results
* Investigate discrepancies
 |
| IT Oversight | IT visually verifies that the vendor matches AIM list of assets to be destroyed **{c}** against physical IT assets rendered | * Interview employee(s) who oversee vendor matches
* Visually observe IT vendor oversight
 |
| Visual Verification | Real time, independent IT verification that hardware destruction vendor actually destroys IT assets | * Interview employee(s) who visually verify IT asset destruction
* Visually observe IT asset destruction
 |
| Certificate of Destruction **[1]** | Confirms the right IT assets were appropriately destroyed | * Refer to **{b}** above
* Match AIM list of assets to be destroyed **{c}** against relevant Certificate(s) of Destruction
* Ensure Department Head signed Certificate(s) of Destruction
 |

**[1]** See **Exhibit A** for a Sample Certificate of Destruction.

CRS proposes comparison of these controls against comparable controls that have been implemented by your Company to evaluate whether they support Policy compliance and to identify potential gaps and vulnerabilities. We also propose limited tests of A+ IT data destruction controls as indicated above to independently assess adequacy of design and to determine whether they are operating effectively.

The RFP also establishes that A+ seeks assurance about the following characteristics of the Policy:

* The Policy appropriately aligns with A+ business and IT objectives;
* The Policy supports compliance with relevant laws and regulations; and
* Existing policies, procedures and controls adequately support Policy enactment.

CRS will compare the Policy against the Company’s most current strategic and business plans and assess propriety of alignment, and we will examine the Policy from a compliance perspective to verify applicable laws and regulations have been effectively addressed. We will then compare Policy contents against effective solutions that have been successfully implemented by our clients and those that are deemed “best practices” by other InfoSec industry experts. We will also review related policies, procedures and practices that govern Information Security; Removable Media Usage; Data Classification and Retention; and Physical Asset Inventories and assess whether they sufficiently support adaptation to the behaviors prescribed by the Policy. Finally, CRS will consider whether the A+ has implemented the following types of controls that may further support Policy compliance:

* Incompatible functions are adequately segregated.
* Help Desk tickets are routinely monitored to ensure timely closure.
* Independent oversight of physical IT asset inventories.
* Asset Inventory Management and Help Desk Ticketing systems are independently audited.
* Internal/external audits of compliance with Service Level Agreements.
* Robust employee training and performance management functions.

In the event CRS encounters any significant risks throughout performance of this engagement, we will notify you immediately. Otherwise, we will provide a written report to Executive Management and the Board of Directors upon audit conclusion that contains the results of our review and testing, accompanied by recommendations for improvement (if applicable). An independent consulting division of CRS is also available to assist with implementing such recommendations.

Our mission is to create a long-standing, mutually beneficial professional relationship with your Company. Please be aware that CRS’ CISA and CISSP certified IT Auditors are required to attend ISACA and ISC training so they are up-to-date with evolving IT security industry trends. We are thereby prepared to provide extraordinary, leading edge services at competitive prices. Please refer to **Exhibit B** for a list of our proposed services and associated fees.

Should you have any questions regarding our proposal, do not hesitate to contact me at (555) 123-4567. In the meantime, thank you providing the opportunity for CRS to submit this competitive bid. We look forward to receiving an affirmative response.

Very Truly Yours,

Jason Wulf

Jason Wulf, C|CISO, CISA/M, CIPT, CISSP

Executive Director, Business Development

CRS InfoSec Solutions

**Exhibit A – Sample Certificate of Destruction**

The information described below was destroyed in the normal course of business pursuant to a proper retention schedule and destruction policies and procedures.

Date of Destruction:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Description of hardware destroyed (e.g. serial #’s, asset barcodes):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Method of destruction:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Destroyed By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Witnessed By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Department Head:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Exhibit B – CRS’ Proposed Services and Related Fees**

CRS InfoSec Solutions will provide the following assurances to A+ Corporation regarding the Company’s newly implemented IT Data Destruction Policy:

* The Policy is sufficiently robust, is aligned with Information Security objectives, and supports compliance with relevant laws and regulations;
* Appropriate compliance enforcement and monitoring mechanisms exist;
* Existing policies, procedures and controls adequately support Policy enactment; and
* Employees/contractors/third parties are complying with the Policy (.

Estimated hours to complete: 60

Blended Rate: $225

Proposed Fees $13,500

Less: 10% New Customer Discount **[2]**  ($1,350)

Net Estimated Fees **$12,150**

**[2]** This discount is non-transferable and only applies to the first Statement of Work executed by and between A+ Corporation and CRS InfoSec Solutions. Offer expires December 31, 2016.