City of Columbus

Secure Email Gateway and Services

RFQ 010244

October 10, 2018

Digital

CDW Government LLC
230 N. Milwaukee Ave.
Vernon Hills, IL 60061

CDW·G PEOPLE WHO GET IT

One CDW Way
230 N. Milwaukee Ave
Vernon Hills, IL 60061

P: 847.371.5800
F: 847.465.6800
Toll-Free: 800.808.4239

www.cdwg.com/PeopleWhoGetIT

City of Columbus
Department of Technology
90 W. Broad St.
Columbus, Ohio 43215

September 27, 2018

RE: Secure Email Gateway and Services RFQ 010244

Dear Mr. H. Samuel Orth III,

The City of Columbus ("City") seeks a qualified vendor to assist with the purchase of a new secure email gateway solution, which will replace the City's current McAfee Email Gateway environment. CDW Government LLC ("CDW•G"), **headquartered in Vernon Hills, IL with a FEIN of 36-4230110**, understands the scope of this project and will continue to serve as a strong partner to the City for this contract. **Our CDW•G proposed solution is based on the implementation of a Proofpoint Threat Protection Suite and is valid for 180 days.**

By continuing to select CDW•G as your trusted partner, the City will enjoy the following advantages:

Best of Breed Solution: CDW•G has partnered with Proofpoint who Gartner considers as the leader of the Magic Quadrant for Secure Email Gateways in 2018. Proofpoint's approach to providing dynamic classification and control of email, multi-layered threat protection, flexible policy creation and detailed reporting are the basis for this award winning solution.

Strategic Partnerships and Extensive Resources: CDW•G's strong partnerships with not only Proofpoint but other leading hardware and software manufacturers will allow us to leverage other solutions that integrate seamlessly with your Proofpoint Secure Email Gateway. With over 1,300 manufacturer partners, we can help the City streamline the procurement process and save you money, time, and effort.

This proposal, **prepared by your Field Rep Nick Geiser,** demonstrates the ways we can successfully continue to meet your technology requirements for hardware, software and implementation services for data center network refresh. **If you have any inquiries regarding our proposal, please contact Nick Geiser at any time either by phone at (614) 318-9058 or via email at nickgei@cdwg.com**. We thank you in advance for your favorable consideration and look forward to our continued collaboration.

Sincerely,

Nicholas Geiser
Field Account Executive

Table of Contents

Response Section 2: Competence

Offeror Profile and Demographics

The Offeror shall demonstrate through its background and staff qualifications that it meets the requirements stated in Section 3.2.1 of this RFP and is capable of providing the services described in this RFP. The Offeror shall clearly show compliance to these minimum qualifications. The RFP Coordinator may choose to determine minimum qualifications by reading that single document alone, so the submittal should be sufficiently detailed to clearly show how you meet the minimum qualifications without looking at any other material. Those that are not clearly responsive to these minimum qualifications shall be rejected by the City without further consideration. The Offeror shall demonstrate this by submitting the following information in its response:

Brief History of CDW Government LLC ("CDW•G")

Founded in 1984, CDW is an innovative leader in multi-brand technology solutions that provides hardware, software, services and integrated solutions to business, government, education, and healthcare organizations. **Headquartered in Vernon Hills, IL,** the company generates $15.2 billion (2017), ranks at 189 on the Fortune 500 list.

In 1998, CDW recognized the need for dedicated support to our government and education customers and created CDW Government ("CDW•G") specifically for this purpose. In 2005, the company consolidated our healthcare customer practice within CDW•G as well. Over the course of the next decade, we have opened locations across the country including a distribution center in Las Vegas, NV in 2005 and an Enterprise Command Center in Vernon Hills in 2015. We own and operate our distribution facilities, which ensures available stock and lower lead times, though we retain the flexibility of leveraging distribution partners to maximize access to IT solutions. Most of our competitors do not have the facilities to provide this value to customers. Our convenient distribution centers, range of products and services, and lower lead times will translate into efficiency, expediency, and reliability, saving the City valuable time and resources. We maintain 24 regional sales offices throughout North America and can truly provide nationwide coverage unlike some of our competitors who either do not carry the full range of products or services or are regionally concentrated.

Company Experience History/Facts:

The offeror must submit an outline of its experience and work history delivering secure email gateway solutions for the past five years.

Products and Resources will be used to meet the City's Requirements

As the largest Value-Added Reseller (VAR) in North America, CDW•G sells more than 100,000 products from over 1,300 Original Equipment Manufacturers (OEMs) to approximately 100,000 government and educational institutions. Our vast partner network enables us to deliver value and performance through innovative solutions that support customers' unique requirements; rather than imposing a single brand on our customers, we arrive at solutions that best address customers' objectives through creative and critical approaches that utilize products across a broad spectrum.

Drawing on 20 years of experience, our over 250 Security experts have orchestrated security solutions for organizations of all sizes in every industry. This robust security practice includes an array of industry certifications like the ones listed below:

We also rely on strong partnerships from the industry leaders in security technology solutions like Email Security. In this security technology set, we are proud to collaborate with Proofpoint. Proofpoint is a Gartner recognized leader in cybersecurity. To date, Proofpoint has over 50,000 customers, processing up to 10 Billion messages a day. Over 60% of fortune 500 companies currently utilize Proofpoint's Secure Email Gateway. Proofpoint successfully deploys thousands of secure email gateways per year, across every vertical (State/Local Government, Retail, Higher Education, Banking, Healthcare, and Technology).

The offeror must submit evidence of financial stability with an annual report, Form 10-K or audited financial statement.

Due to page restrictions and to ensure you have access to the technical sections of our proposal, we are providing the City with a link to our financial statements. You will have access to all our 10-K reports and to the most recent corporate annual report. The City can visit the following Web address to access the report: http://investor.cdw.com/sec.cfm

The offeror must submit the name/location of a technical support center that provides remote services.

Proofpoint delivers support at two U.S Locations:

1. 892 Ross Drive Sunnyvale, CA 94089

2.13997 South Minuteman Drive Suite 300 Draper, UT 84020.

The offeror must provide a description for each labor classification to include minimum education, training, and/or certifications, average years of experience, typical promotion track and typical responsibilities.

CDWG interprets this request to be related to the implementation resources required. Proofpoint will be providing the implementation of this solution and will provide resumes of prospective resources upon award.

The offeror may provide any pertinent facts not explicitly requested.

Response Section 3: Quality & Feasibility

The Offeror's technical proposal shall address the requested services described in Section 3.3 of this RFP by submitting the following information in its response:

Complete description of the secure email gateway product capabilities and features proposed including:

5.3.1.1: Powered by the patented Proofpoint MLX machine learning technology, Proofpoint spam and phishing technology efficiently filters millions of possible attributes in every email. This advanced level scanning protection accurately filters emails by examining envelope headers and structure, content, email sender reputation, images and more, to prevent spam emails, malware, other malicious email and attachment-based spam reaching inboxes.

5.3.1.2: Proofpoint provides granular filtering to control bulk "graymail" or marketing and other unwanted email.

5.3.1.3: Proofpoint Target Attack Protection is built on our next-generation email security platform, which gives you a unique architectural advantage. You get clear visibility into all email communications for a far-reaching view of the threat landscape. See everything from banking trojans and ransomware to attacks targeted at your organization. Deep, message-level context makes TAP especially effective at identifying hard-to-catch threats those other solutions miss.

5.3.1.4: Proofpoint Email DLP works toward preventing organizations' employees from leaking sensitive corporate data through email, either accidentally or intentionally. The product's Smart Send tool doesn't simply block outbound emails, but allows users to remediate policy violations and educates them on the specifics of the security policy. In addition, built-in, policy-based email encryption allows for the exchange of sensitive data with customers and business partners, and the Digital Asset Security feature and managed dictionaries provide automatically updated policies.

5.3.1.5: With Proofpoint Email Encryption, messages and attachments are automatically encrypted with complete transparency. Users don't need to manually encrypt their email to send and receive messages securely. All email encryption policies are centrally managed and enforced at the gateway. A convenient graphical interface helps you define email encryption policies, which can be triggered by messages containing regulated information or intellectual property.

5.3.1.6: Email Protection gives you a wealth of data and search tools. Our advanced message tracing features a high-performance search engine to help you quickly pinpoint hard-to-find log data based on dozens of search criteria. With more than 60 real-time reports for detailed visibility into mail flow and trends, Email Protection provides the data that can help address issues and trends as they emerge.

5.3.1.7:

- Proofpoint's LDAP integration enables you to set policies based on any LDAP attribute, for any individual, group, division, and more.
- Proofpoint offers the best protection for Office 365 & Microsoft Exchange. We secure your people and data with superior protection against threats and compromised accounts. And we provide curated threat intelligence and deep forensics. We help your IT team provide a great end-user experience.

- Proofpoint owns and operates the world's foremost threat intelligence database, Proofpoint product are intended to leverage this technology.
- Proofpoint Target Attack Protection would offer the ability to sandbox attachments and URL's. This functionality would replace existing McAfee deployment.
- The Proofpoint and Splunk partnership provides security teams a unified way to view insider threats, determine the lateral spread of threats and get visibility into data exfiltration.

5.3.1.8 - Proofpoint offers comprehensive and intuitive management interface

5.3.1.9 - Proofpoint offers easy to use and fully customizable end user interface.

5.3.2: **Complete description of the proposed secure email gate product architecture including:**

5.3.2.1: - Proofpoint Enterprise Protection can be deployed in unique hybrid configurations

5.3.2.2: -Proofpoint has the ability to deploy Role based access controls over multiple users containing multiple roles. Scoping of roles can be very granular within the product.

5.3.2.3: - Proofpoint provides for best practices to deploy a secure and hardened configuration.

5.3.2.4:-Proofpoint offers a sub-organization feature to allow multi-tenant and multi-domain configuration within the product.

5.3.2.5:-Proofpoint systems have the ability to scale significantly beyond 10,000+ email users, 100,000 incoming emails per day & 10,000+ outbound emails.

5.3.3: **Description of the offerors plan to deliver services described in section 3.3.3 including.**

5.3.3.1: Proofpoint Professional Service and delivery team will work with the City of Columbus to perform installation and network integration to industry best practices.

5.3.3.2: **Integrations with:**

5.3.3.2.1: Proofpoint Professional Services and delivery team will work with the City of Columbus to integrate the city's LDAP infrastructure into the Proofpoint solution.

5.3.3.2.2: Proofpoint Professional Services and delivery team will work with the City of Columbus to configure Proofpoint solutions to work seamlessly with the City's current Microsoft Exchange infrastructure.

5.3.3.2.3: Proofpoint is offering solutions and capabilities that would supersede the need to continue to maintain McAfee TIE and ATD.

5.3.3.2.4: Proofpoint Professional Services and delivery team will work with the City of Columbus to configure Proofpoint solutions to work seamlessly with the City's current Splunk infrastructure. Proofpoint is a Splunk certified security partner and currently maintains several certified TA's.

5.3.3.3: Proofpoint Professional Services will work with the City of Columbus to discuss configuration best practices for policy creation, assist with policy creation, deploy policies, and finally test & tune policies once in production.

5.3.3.4: Proofpoint Professional Services will assist with the entire live production cutover and any support issues that arise at that time. Once a stable production environment has been established, Proofpoint will continue to provide ongoing support through the Proofpoint Customer Support Center through the included Platinum support contract quoted here.

5.3.3.5: as a part of our proposal, we have included two instructor led onsite training courses. We are also including self-paced virtual training through our Proofpoint University Platform.

In addition to the specific narratives for Section 5.3, we also wanted to provide our narratives related to sections 3.3: Solution Requirements:

3.3.1.1: - Proofpoint MTA complies with the latest published standards and provides granular control

3.3.1.2: - Traditional inbound/outbound anti-spam and anti-malware capabilities such as:

- Proofpoint has signature based and heuristic detection anti-malware and virus scanning
- Proofpoint has the ability to detect suspicious based on reputation, and the ability to block or prevent the messages from being delivered

3.3.1.3:- Marketing and graymail classification capability such as:

- Proofpoint has the ability to separate SPAM from graymail into separate quarantines using our Bulk mail classifier. This can be accomplished on a personalized and granular policy level and provided to end users for control as well.
- Proofpoint has a safe unsubscribe feature

3.3.1.4:- Advanced Threat & targeted attack defense including post-delivery protection such as:

- Proofpoint provides deep context and file inspection
- Proofpoint has the capability to Sandbox malicious messages, detonate payload, and follow the URL link
- Proofpoint sandboxing efficacy is such that CDR type technologies are not necessary within our product set.
- Proofpoint does rewrite URLs and analyze messages at time of click, for deep URL based threat defense
- Our unique predictive analysis preemptively identifies, and sandboxes suspicious URLs based on email traffic patterns. This drastically minimizes the risk of a patient-zero case from a previously unknown malicious URL.
- Proofpoint's sandboxing environment does perform static memory exploit detection.
- Proofpoint's Email Fraud Defense 360 solution does provide protection from BEC as well as provide data on domain name look-alike threats typically referred to as "cousin domain" threats. Proofpoint's SEG provides protection against display name spoofing and has an imposter classifier built in to protect against imposter-based threats.
- Proofpoint's Threat Response Auto Pull (TRAP) tool provides for eradication of malicious and noncompliant email from the mail store (on-prem and cloud-based mail stores).
- Proofpoint has the capability to give email recipients a notification of the trust-ability of the email sender based on several factors customizable by the administrator.
- Proofpoint cloud-based pre-filter delivers effective Anti-Spam protection against new and emerging spam techniques.

3.3.1.5:-Data Loss Prevention for outbound content including features such as:

- Proofpoint Email DLP comes "out of the box" with predefined policies to look for all standard forms of restricted content, such as PCI, HIPAA, FINRA and other regulated material using a multi layered approach combining traditional dictionaries with Proofpoint Smart Identifiers.
- Proofpoint Data Loss Prevention is easy to administer and use for a compliance officer.
- Proofpoint scans all documents for active content via our world-class sandboxing environment to determine if a document is truly malicious. We then take the appropriate action based on this verdict returned from the sandboxing environment.
- Proofpoint does not currently have the ability to perform image level detection.

- Using Proofpoint's Digital Assets module built into our strong DLP engine we are able to detect protected and/or proprietary data deemed a digital asset by the customer. The threshold for detection of drip DLP data is customizable by the administrator in the policy.

3.3.1.6:- Native policy based, push and or pull encryption email encryption methods beyond TLS for outbound content such as:

- Proofpoint allows an individual message to a specific recipient can be revoked without affecting other users or other messages to the same recipient
- Read receipts are built into the Proofpoint Encryption Solution
- All messages can be set with specific expiration based on policy
- Proofpoint provides end users the ability to send large files, and files that require enhanced security
- Proofpoint supports a very wide range of file formats
- Proofpoint's Encryption Service provides a web based secure reader inbox for reading encrypted messages on a wide range of desktop and mobile platforms

3.3.1.7:- Strong Reporting capabilities such as:

- Proofpoint Targeted Attack Protection (TAP) provides some of the industry's best security reporting available. Through the wealth of information gathered by our world class threat research team we are able to provide immense detail and individual and campaign level threats, deep forensic data into all our detections, detailed information on the end user base and behavior, as well as profiling of attackers and attacks being targeted at your organization
- Proofpoint has capabilities to rate risky user behaviors that are known to be predicative of an insider threat through our comprehensive Cloud Account Defense Suite, which can be additionally licensed.
- Proofpoint reporting provides industry, vertical, geographic, and other comparisons as well as comparisons against best practice security metrics
- Proofpoint provides Granular Ad-Hoc reporting
- Proofpoint's reporting experience is driven by our world class threat research and the reporting follows the same standard being analytics driven
- All fields in the reporting sections of TAP are clickable to drill down into fine grained granular reporting on the higher level attributes
- Administrators can customize their individual dashboard

3.3.1.8: - Integrations with related technologies such as:

- LDAP - Yes
- Microsoft Exchange & Office 365 - YES
- Proofpoint can integrate with ATD; however, Proofpoint's Targeted Attack Protection solution will act as a replacement for McAfee ATD.
- Splunk Enterprise Security - Proofpoint has a deep and strategic partnership with Splunk that provides security teams a unified way to view insider threats, determine the lateral spread of threats and get visibility into data exfiltration. We have direct connectivity and several certified TAs available for use as a free integration

3.3.1.9:- Intuitive easy to use management interfaces with features such as:

- Proofpoint's on premises solution operates in a single portal, Proofpoint cloud hosted product operate in a single portal.
- Proofpoint is actively working to standardize all solutions across a modern HTML5 interface.
- Proofpoint's interface supports context sensitive and robust help functions on every page
- Proofpoint has limited support for individual widgets today and we are actively adding more broad support for widgets in future releases.
- Proofpoint has very extensive and granular policy control natively built into every module
- Proofpoint systems provide granular audit and log management

3.3.1.10:- Intuitive easy to use interfaces with features such as:

- Proofpoint gives the ability to easily manage quarantined messages both from an administrator's point of view as well as an end user's perspective.
- Big data analysis techniques accurately identify graymail and marketing messages and deliver it to a separate low-priority inbox
- Proofpoint provides a secure reader inbox interface to easily and seamlessly manage encrypted emails

3.3.2:- Architecture, Capacities, and Licensing requirements:

3.3.2.1: - Proofpoint architecture offers on prem or hybrid environments (premise/cloud). We will offer a design that provides full resiliency between two on premise sites

3.3.2.2: - Proofpoint allows for Role Based Administration

3.3.2.3: - Proofpoint deploys a secure & hardened configuration

3.3.2.4: - Proofpoint will support multitenant/multi domain environments

3.3.2.5: - Capacity and Licensing

- Can support 10,000+ email users
- Can support 100,000+ emails per day
- Can support both domains sending 9,600+/day
- Included in pricing document

3.3.3.1: -Proofpoint will provide a project manager to coordinate City and Services Tasks

3.3.3.2: -Solution design and Project plan: Deliver a complete solution design and project plan, including:

- An example project plan is included with this proposal; a specific project plan will be created, customized, and coordinated between the City of Columbus and Proofpoint Professional Services after contract is awarded. This plan will be specific and based on all specifications provided by the City of Columbus to Proofpoint. The plan will include a detailed design to include:
    - Network connectivity and data flows between the City of Columbus and Proofpoint products/solutions
    - Systems Security Plan including Access Management and control, based on City of Columbus requirements
    - Detailed plan to Integrate Proofpoint solution with City of Columbus LDAP infrastructure, Exchange mail servers, and deploy Splunk certified TAs
    - Policy design reflecting best practice for effective email security and selective translation of existing city policies.

3.3.3.3: - Two training courses included in proposal

3.3.3.4: - Solution testing and implementation: Perform necessary steps for solution implementation including:

- No Hardware
- Proofpoint will deploy the most recent and fully supported version
- Software configuration will adhere to Proofpoint's best practices.
- Proofpoint will work with the City of Columbus to discuss integrations where needed and perform tasks around these integrations.
- Proofpoint will work with the City of Columbus to implement policies based on city needs and Proofpoint best practices

3.3.3.5- **Go Live Support-** Proofpoint offering includes Go-live and post Go-live support.

3.3.3.6: - Proofpoint has included DMARC implementation through our Email Fraud Defense solution, which is included in the proposal.

Response Section 4: Availability

CDWG is one of Proofpoint's top resellers and we have utilized our breadth of resources to be able to support customer's security initiatives. As mentioned previously, CDWG has over 250 security experts that develop and security solutions for customers.

These security solution sets include penetration testing for internet, internal, wireless, application security, social engineering, and red teaming scenarios. We locate the gaps in your security with services that range from cost effective scanning to detailed and comprehensive analyses. These assessments are performed by skilled engineers and can be tailored to meet your organization's needs.

Having been established for over 30 years, CDW has an excellent track record of financial performance that provides peace of mind for our customers. Headquartered in Vernon Hills, IL with over 20 locations in the United States, most of all our resources are located in the United States. At CDW, most of our security services are performed by in-house professionals with expertise in a range of technical disciplines and products. Many of our engineers have more than a decade of individual experience in military, government and private-sector work. Additionally, our security staff maintain numerous certifications, including Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), Offensive Security Certified Professional (OSCP) and SANS Global Information Assurance Certification (GIAC).

With this particular solution and partnership with Proofpoint, we have chosen to lean on their badged resources for the implementation of the solution. We specifically have Proofpoint perform the services because they are most intimately aware of the proper configurations that ensure a successful project.

This packaged service provides the requirements that the City of Columbus has outlined in their request. In addition, Proofpoint is willing to provide this service at no charge to the City of Columbus. The details of this service are included in the Additional information section of our proposal. We look forward to discussing this with you and confirming that you are getting the implementation services that you desire.

In terms of the calendar, below is a sample of the calendar that is used as a part of the implementation. Due to the constraints on the proposal size, we have also included a more robust calendar in the Additional Information section.

Outline Level	ID	Name	Predecesso	Resource Names	Status	T
1	1	**Initiate and Plan**				
4	2	Gather Customer Requirements		Proofpoint City of Columbus CDW		
4	3	Conduct Kick-Off meeting.		Proofpoint City of Columbus CDW		
4	4	Confirm Receipt of Welcome Letter		Proofpoint City of Columbus CDW		
4	6	Schedule standing project status/working meetings		Proofpoint City of Columbus CDW		
4	7	Review Architecture with City of Columbus		Proofpoint City of Columbus CDW		
4	9	Provide product documentation		Proofpoint		
4	11	Confirm milestone target timelines with City of Columbus		Proofpoint City of Columbus CDW		
1	12	**Design and Configure**				
2	13	System Set Up and System Configuration				
3	14	Implement firewall rule changes based on Proofpoint Firewall Matrix		City of Columbus		
3	27	Proofpoint on Demand (PoD) Provisioning and Setup		Proofpoint		
4	28	Validate Proofpoint on Demand (PoD) Provisioning		Proofpoint		
4	29	Reassess Proofpoint on Demand (PoD) Sizing	28	Proofpoint		
4	30	Run Health Check Script prior to configuration IF POC took place on the cluster	28	Proofpoint		
3	38	User Imports: LDAPS Configuration		Proofpoint City of Columbus CDW		
4	39	Create Active Directory account for LDAPS access from PPS	14	City of Columbus		
4	40	Configure LDAPS user imports and verify synchronization	39	Proofpoint		
3	41	User Imports: Azure AD		Proofpoint City of Columbus CDW		
4	42	Provide Azure configuration document		Proofpoint		
4	43	Create Azure Application and provide configuration data from output (tenant id, client id, key)	42	American Tower		
4	44	Create import/auth profile on PPS	14 and 43	Proofpoint City of Columbus CDW		
4	55	Schedule user imports to run on a regular interval	54	City of Columbus		
3	60	Administrative Configuration		Proofpoint City of Columbus CDW		
4	61	Administrator Roles/Accounts	19 or 25 or 28	Proofpoint City of Columbus CDW		
4	62	Set up System Alerting	19 or 25 or 28	Proofpoint City of Columbus CDW		
2	63	Protection Configuration (Inbound)				
4	64	System Module Configuration - Add Domains, SMTP Profiles, Policy Routes, TLS	2 and 14	Proofpoint City of Columbus CDW		
4	65	Virus Protection Module Configuration	2 and 14	Proofpoint City of Columbus CDW		
4	66	Spam Detection Module Configuration - including SCSS, Imposter, Low Priority	2 and 14	Proofpoint City of Columbus CDW		
4	67	User Management Module Configuration - Apply Inbound Spam Policy	66	Proofpoint City of Columbus CDW		
4	68	Email Firewall Module - SPF, DKIM, Max Size	2 and 10	Proofpoint City of Columbus CDW		
4	69	End User Services Module End User Web Configuration	55	Proofpoint City of Columbus CDW		
4	70	End User Services Module: provide company logos for use in digest branding		City of Columbus		
4	71	End User Services Module: Configure and verify user digests including branding	55	Proofpoint City of Columbus CDW		
4	72	Provide email feedback plugin information		Proofpoint		
2	73	Targeted Attack Protection Configuration				
4	74	Setup TAP administrators and alerts		City of Columbus		
4	75	Review TAP Dashboard		Proofpoint City of Columbus CDW		
4	76	Review TAP API SIEM Info and Configuration		Proofpoint City of Columbus CDW		
3	77	TAP SaaS Defense Configuration	2 and 10	Proofpoint City of Columbus CDW		
4	78	Provide documentation for TAP SaaS Defense		Proofpoint		
4	79	Create Service Account for TAP SaaS Defense		City of Columbus		
4	80	Enable API		City of Columbus		
4	81	Notifiy Proofpoint tasks are complete	80 and 81	City of Columbus		
4	82	Email Developer that API is enabled		Proofpoint		
3	83	TAP URL Defense Configuration	2 and 10	Proofpoint City of Columbus CDW		
4	84	Provide block page customization and/or branding information		City of Columbus		
4	85	Submit ticket for block page	83	Proofpoint		
3	86	TAP Attachment Defense Configuration	2 and 10	Proofpoint City of Columbus CDW		
2	87	Protection Configuration (Outbound)				
4	88	System Module Configuration - Allow Relay, Policy Routes, TLS	2 and 14	Proofpoint City of Columbus CDW		
4	89	Spam Detection Module Configuration	88	Proofpoint City of Columbus CDW		
4	90	User Management Module Configuration - Apply Outbound Spam Policy	89	Proofpoint City of Columbus CDW		
4	91	Virus Protection Module Configuration	88	Proofpoint City of Columbus CDW		
4	92	Email Firewall Module - SPF, DKIM, DMARC, Non-throttled hosts	88	Proofpoint City of Columbus CDW		
4	93	Check SPF records and update if necessary	2	Proofpoint City of Columbus CDW		
2	94	Encryption Configuration				
4	95	Create CNAME (PoD) or A record (on-prem) for use with Proofpoint Encryption		City of Columbus		
4	96	Import Certificate for Secure Reader	13	City of Columbus		
4	97	Assign certificate to SR service for all SR agents	13	City of Columbus		
4	98	Configure General Encryption Settings including FQDN	13	Proofpoint City of Columbus CDW		
4	99	Configure Encryption Branding Template	13	Proofpoint City of Columbus CDW		
4	100	Review Encryption options	13	Proofpoint City of Columbus CDW		
4	101	Configure Encryption Settings	13	Proofpoint		
4	102	Enable EFW rules for Encryption	101	City of Columbus		
4	103	Provide Encryption plugin information		Proofpoint		
2	104	DLP Configuration				
4	105	Gather Regulatory Compliance Requirements		City of Columbus		
4	106	Review requirements and configure applicable default rules and dictionaries for audit	105	Proofpoint City of Columbus CDW		
4	107	Create additional custom dictionaries and rules to meet requirements (as applicable) for audit	106	Proofpoint City of Columbus CDW		
2	108	Remote Syslog Forwarding Configuration				
4	109	Provide trusted CA Certificate		City of Columbus		
4	110	Import trusted CA Certificate	109	Proofpoint City of Columbus CDW		
4	111	Import and Apply Certificate to Syslog Forwarding Client	110	City of Columbus		
4	112	Configure remote server details and Test Connection	111	Proofpoint City of Columbus CDW		
4	113	Configure log types and enable	112	Proofpoint City of Columbus CDW		
2	139	Threat Response Auto Pull Configuration				
4	140	Set up a virtual machine for TRAP	14	City of Columbus		
4	141	Assign a service account	14	City of Columbus		
1	142	**Test**				
4	143	Provide sample **Test Plan**		Proofpoint		
4	144	Run Health Check Script	12	Proofpoint		
4	145	Create Test Plan		City of Columbus		
4	146	Execute Test Plan		City of Columbus		
2	147	DLP Testing				
4	148	Review DLP audit results	107 and 192	Proofpoint City of Columbus CDW		
4	149	Fine tune DLP rules based on audit findings	148	Proofpoint City of Columbus CDW		
1	156	**Enable**				
2	159	Training and Communication				
3	160	Develop and Initiate Administrator Training and Communication		Proofpoint City of Columbus CDW		

Options for
- Leave blank
- In Progress
- On Track
- Off Track
- Complete
- Out of Scop

Response Section 5: Past Performance

Company Name: Nationwide Children's Hospital	**Contact Name:** Brad Salt **Contact Title:** System Engineering Manager
Company Address: 700 Children's Drive Columbus, OH 43205 United States	**Contact Phone Number:** 614.355.3809 **Contact Email Address:** brad.salt@nationwidechildrens.org
Project Name: Email Security	**Beginning Date of Expr: /Ending Date of Expr:** **Month/Year** **Month/Year** 12/2015-12/2018
Number of Domains: Multiple **Number of Mailboxes:** 8,000	**Solutions:** Secure Email Gateway, Target Attack Protection, adding Threat Response and Email Fraud Defense

Company Name: University of Toledo	**Contact Name:** Jason Rahe **Contact Title:** Sr. Systems Collaboration Mgr.
Company Address: 2801 W Bancroft St Toledo, OH 43606-3390 United States	**Contact Phone Number:** 419-530-3161 **Contact Email Address:** jason.rahe@utoledo.edu
Project Name: Email Security and compliance	**Beginning Date of Expr: /Ending Date of Expr:** **Month/Year** **Month/Year** 9/2017-10/7/2018
Number of Domains: Multiple **Number of Mailboxes:** 27,500	**Solutions:** Secure Email Gateway, Target Attack Protection, Threat Response, DLP/Encryption, Email Fraud Defense

Company Name: City of Detroit	**Contact Name:** Mike Homant **Contact Title:** Director, Enterprise Technology Ops
Company Address: 2 Woodward Avenue Suite 1126 Detroit, MI 48226 United States	**Contact Phone Number:** (313) 224-2589 **Contact Email Address:** mike.homant@detroitmi.gov
Project Name: Email Security	**Beginning Date of Expr: /Ending Date of Expr:** **Month/Year** **Month/Year** 5/2018-5/2019
Number of Domains: Multiple **Number of Mailboxes:** 9,300	**Solutions:** Secure Email Gateway, Targeted Attack Protection

Response Section 6: Terms & Costs

5.6.1: Terms and Conditions

CDW Government LLC (CDWG) is submitting this proposal with the understanding that except with respect to the product, quantity, and price specifications included in this response, that the terms and conditions of the City of Columbus Contract pursuant to the Video Storage Specs (RFQ004361), effective May 18, 2017, and not any terms contained in the underlying RFP, will govern any resulting transaction. CDWG is open to negotiating these or any other terms and conditions upon award.

With regard to third party cloud computing and storage services, CDWG acts as a rebiller only. The City of Columbus, OH ("Customer") acknowledges that Customer, and not CDWG, will be responsible for performance of the Cloud Services. Customer must execute CDWG's Cloud Service Order form before purchasing cloud computing and/or storage services. In addition, before CDWG can sell cloud computing and/or storage services from a third party to Customer, Customer must execute an agreement governing said cloud computing and/or storage services with the third party cloud services provider. CDWG has included a sample Proofpoint Cloud Service Order Agreement in the Additional Information Section.

5.6.2: Costs

Below are the costs for a 1-year term - $334,731.40:

Qty.	Part #	Description	Term	Unit Price	Extended Price
	Proofpoint Solution - 1YR Term				
12377	PP-B-TBEPF-V-A-109	Targeted Attack Protection URL Defense & Attachment Defense, Dynamic Reputation, Spam, Virus Protection, Zero- Hour Anti-Virus, Email Firewall, Smart Search - F-Secure - Virtual	12 Mo	$13.00	$160,901.00
12377	PP-B-DLPE-V-A-109	Regulatory Compliance, Digital Asset Security, Encryption - Virtual	12 Mo	$5.20	$64,360.40
12377	PP-A-EFD360L-S-A- 105	DMARC deployment for up to 5 sending domains (and unlimited defensive registrations). Defend against all email fraud tactics used in an organization's email ecosystem (domain spoofing, display name spoofing and the use of look-	12 Mo	$5.00	$61,885.00
1	PP-SUP-PS-12	Platinum Level Support	12 Mo	$22,708.00	$22,708.00
	Proofpoint Solution - Implementation				
1	PP-PST-EITPB-A-102	Proofpoint Platform (MTA) with Email Protection, Information Protection and Targeted Attack Protection Configuration (SaaS or On-Premise Appliance)		$0.00	Included
1	PP-PST-EFD-INT-102	Proofpoint EFD Initial Configuration		$0.00	Included
	Proofpoint Solution - Training				
2	PP-PCA-INPRO-OS- 102	ILT, Customer Onsite / 2 days /$4000.00/day/ upto 10 students maximum.		$6,219.00	$12,438.00
2	PP-PCA-PRO-OS-102	ILT, Customer Onsite / 2 days /$4000.00/day/ upto 10 students maximum.		$6,219.50	$12,439.00
				Grand Total:	**$334,731.40**

Below are the costs for a 3-year term - $911,549.40:

	Qty.	Part #	Description	Term	Unit Price	Extended Price
		Proofpoint Solution - 3YR Term				
	12377	PP-B-TBEPF-V-A-309	Targeted Attack Protection URL Defense & Attachment Defense, Dynamic Reputation, Spam, Virus Protection, Zero- Hour Anti-Virus, Email Firewall, Smart Search - F-Secure - Virtual	36 Mo	$37.00	$457,949.00
	12377	PP-B-DLPE-V-A-309	Regulatory Compliance, Digital Asset Security, Encryption - Virtual	36 Mo	$14.00	$173,278.00
	12377	PP-A-EFD360L-S-A- 305	DMARC deployment for up to 5 sending domains (and unlimited defensive registrations). Defend against all email fraud tactics used in an organization's email ecosystem (domain spoofing, display name spoofing and the use of look-	36 Mo	$15.00	$185,655.00
	1	PP-SUP-PS-12	Platinum Level Support	36 Mo	$70,238.00	$70,238.00
		Proofpoint Solution - Implementation				
	1	PP-PST-EITPB-A-102	Proofpoint Platform (MTA) with Email Protection, Information Protection and Targeted Attack Protection Configuration (SaaS or On-Premise Appliance)		$0.00	Included
	1	PP-PST-EFD-INT-102	Proofpoint EFD Initial Configuration		$0.00	Included
		Proofpoint Solution - Training				
	2	PP-PCA-INPRO-OS- 102	ILT, Customer Onsite / 2 days /$4000.00/day/ upto 10 students maximum.		$6,107.00	$12,214.00
	2	PP-PCA-PRO-OS-102	ILT, Customer Onsite / 2 days /$4000.00/day/ upto 10 students maximum.		$6,107.70	$12,215.40
					Grand Total:	**$911,549.40**

Additional Information

Please see the following additional documents on subsequent pages:

- CDW•G's Cloud Service Order Agreement
- Proofpoint Services Description

CDW Customer Service Order Form

Proofpoint

Terms:

TERMS AND CONDITIONS - Customer's obligations under this Customer Service Order Form, including its payment obligations are subject to the current Third Party Cloud Services Terms and Conditions on Seller's website at Third Party Cloud Services Terms and Conditions, unless Customer has entered into a written agreement with Seller covering Customer's purchase of products and services from Seller ("Existing Customer Agreement"), in which case Customer's obligations shall be subject to the terms of such Existing Customer Agreement.

SUBSCRIPTION TERM START DATE – The subscription term will start on the date that Proofpoint activates the applicable Cloud Service.

PAYMENT – Customer will pay all Fees (as defined herein) for the use of the Cloud Services and the implementation services as set forth in Seller's invoice ("Implementation Services"), within 30 days after the date of the invoice, or in accordance with such other payment terms that may have been negotiated between Customer and Seller. In addition to the Service Fee for the Cloud Services and the Implementation Services, Customer will also be responsible for all additional fees for any subscription renewals and extensions, metered usage components consumed by Customer, and other subscriptions, features, products, services, or add-ons that Customer uses within the Cloud Services. Seller will invoice Customer in advance for the monthly or prepaid charges due for the Cloud Services purchased. Seller will invoice Customer on a one-time basis, in advance for the Implementation Services. Seller will invoice Customer in arrears for any metered usage or overage components (e.g., capacity overages, third party content, etc.). The Service Fee for the Cloud Services and the Implementation Services and all additional fees due hereunder are collectively referred to as "Fees".

ADD-ON ORDERS - Any orders submitted by Customer to Seller for Proofpoint Cloud Services (and any associated Implementation Services) over the next twelve (12) months (the "Add-On Order(s)") will be governed by the terms and conditions of this Customer Service Order Form. All Add-On Order(s) must include the name of the applicable Proofpoint Cloud Service, any associated Implementation Services, the Licensed User Quantity and the length of the initial term (e.g., 1, 2, or 3 years). The Initial Subscription Term for any Add-On Order(s) will commence on the date Seller provisions the new Proofpoint Cloud Services on behalf of Customer.

NON-CANCELLABLE/NON-REFUNDABLE - The Cloud Services purchased under this Cloud Service Order Form are non-cancellable and all Fees paid to Seller are non-refundable.

SERVICE SUSPENSION – In addition to any other rights Seller may have, Seller may suspend or terminate the Cloud Services if Customer fails to pay any Fees within ten (10) business days after the applicable due date.

BY CLICKING AGREE, Customer acknowledges and agrees that it is receiving the Cloud Services directly from Proofpoint, Inc. ("Proofpoint") pursuant to Proofpoint's standard terms and conditions. Customer further acknowledges that Proofpoint and not Seller will be responsible for performance of the Cloud Services.

proofpoint

Service Brief: Email Protection Information Protection and Targeted Attack Protection Bundle

Professional Services SKU: PP-PST-EITPB

Version 1.0, Last Updated [September 21,2017]

Project Overview

This "***Service Brief***" documents the services that Proofpoint, Inc., through its Professional Services organization or its authorized agents ("***Proofpoint***"), will render to the customer in relation to the implementation of Proofpoint Email Protection and Information Protection ("***Services"***).

This Service Brief is subject to the General Terms and Conditions entered into by Customer and Proofpoint. In the event of any inconsistency between this Service Brief and the General Terms and Conditions, this Service Brief shall govern, but only to the extent of any inconsistency.

Unless otherwise mutually agreed in writing between the Customer and Proofpoint, the Customer's acceptance of the purchase order is considered acceptance of this Service Brief as defined.

See Fixed Bid Service Details for terms and conditions.

For questions concerning this Service Brief contact services@proofpoint.com.

Project Overview

Estimated Engagement Time	3 – 7 Weeks
Maximum Engagement Time	12 Weeks*
Estimated Number of Hours	32-40 Hours
After Hours Work	Not Included
Onsite Work	Not Included
Proofpoint Business Hours	Monday – Friday 9 AM GMT – 2 AM GMT**
Service Brief Expiration	12 Calendar Months (from product purchase)

** Services must be rendered generally within the Maximum Engagement Time. Any extension to this time frame must be approved by Proofpoint Professional Services in writing, and may result in additional charges.*

*** Excluding Proofpoint Holidays.*

proofpoint

Project Scope

Proofpoint personnel, or authorized agents, shall work closely with Customer personnel to perform the services listed under Proofpoint Professional Services Responsibilities, subject to the Customer satisfying the Customer Responsibilities specified herein.

Proofpoint Professional Services Responsibilities

Project Design

- Facilitate project kick-off, planning and status meetings.
- Provide initial project and test plans.
- Review project scope and staffing requirements.
- Review customer requirements and planned use of product features and functions.

Implementation

- Review Network and System Settings
- Assist customer with configuration of product features included with Proofpoint Protection:
  - Email Firewall
  - End User Services
  - Spam Detection and Virus Protection
  - User Imports
- Assist with configuration of purchased product modules included with Proofpoint Targeted Attack Protection:
  - Attachment and URL Defense
- Review TAP (Targeted Attack Protection) Dashboard
- Assist customer with configuration of product features included with Proofpoint Information Protection Suite:
  - Proofpoint Encryption
  - Email Data Loss Prevention (DLP)
    - Regulatory Compliance
    - Digital Asset Security
  - Data Discovery
  - Secure Share
- Assist customer with configuration of mail routing.
- Assist with configuration of user imports via LDAP/LDAPS or Hosted File Transfer.
- Execute unit testing during configuration.

Training and Communication

- Conduct product knowledge transfer with Customer resources during implementation.
- Provide product documentation, support guide and user communication templates.

NOTE: Product knowledge transfer is not a substitute for the formal Proofpoint product customer training courses. Proofpoint strongly encourages completion of Proofpoint Accredited Engineer training.

Production Cutover

- Execute Test Plan and assist customer with inbound and/or outbound email cutover.
- Validate Proofpoint instance is functioning within expected parameters.

NOTE: Unless mutually agreed in writing, all cutover must happen during Proofpoint business hours. Cutover outside of standard business hours may result in additional charges.

Project Closure

- Refine configuration to address any issues following cutover.
- Ensure all project tasks are complete.
- Transition Customer to Proofpoint Support for ongoing product support.

Customer Responsibilities

Project Design

- Complete all items listed in Pre-engagement Checklist provided at project initiation.
- Provide at least one technical resource with system administration responsibilities and appropriate system access privileges.
- Provide network architecture and email flow diagram of Customer's environment.
- Communicate business requirements.

Implementation

- Ensure all relevant resources are available for kick off, planning, configuration and status meetings.
- Ensure vendors and third parties are accessible as necessary during implementation services.
- Assume all responsibility for network connectivity, performance, and configuration issues within Customer environment.
- Implement rules to match configuration from incumbent solution with assistance from Proofpoint.
- Implement branding configuration and settings, with the exception of branding for Proofpoint Targeted Attack Protection and Proofpoint Secure Share.

Training and Communication

- Execute Customer communication plan to notify users of change in service.
- Update processes and procedures to include Proofpoint service and support.
- Complete Proofpoint Accredited Engineer certification training. This is highly recommended for technical resources and required for Proofpoint Authorized Support Users.

Production Cutover

- Customize test plan to meet Customer security and testing requirements.
- Manage Customer change control processes.
- Ensure availability of domain administrators to assist with change of MX records.

Project Closure

- Ensure all project action items are complete.

proofpoint

Fixed Bid Service Details

1. Proofpoint Staffing

Proofpoint provides appropriate onsite and/or offsite personnel (or authorized agents) to perform the Services specified in the Proofpoint Professional Services Responsibilities of the Project Scope section of a respective Service Brief.

2. Materials

The following Proofpoint materials are provided in connection with the Services:

- Pre-engagement Checklist
- Proofpoint sample project plan
- Proofpoint sample test plan
- Product documentation

3. Services Scope Changes

Any changes to the Services, the project schedule, costs of Services, or this Service Brief must be mutually agreed upon by Proofpoint and the Customer in writing. Depending on the scope of such changes, Proofpoint may require that an additional separate Professional Services Statement of Work and/or change order ("***Change Order***") be created and signed by the parties. The Statement of Work and/or Change Order will detail the change, impact of the proposed change on costs/schedule, as well as any other relevant terms to be mutually agreed to in writing.

4. Service Schedule

The anticipated Service start date is a mutually agreed upon start date after receipt and approval by Proofpoint of the Customer's purchase order for the respective Service. Customer shall have twelve (12) months from the date of Proofpoint invoice to use the Services described herein ("***Service Period***"). Proofpoint's obligation to provide the Services shall automatically expire on the last day of the Service Period, unless otherwise agreed by Proofpoint. Under no circumstances shall Customer be entitled to a credit or refund of any unused portion of the Services.

5. Services Scope Exclusions

Proofpoint is responsible for performing only the Services described in this Service Brief. All other services, tasks and activities are considered out of scope, including, but not limited to the following:

(i) Any additional hardware, software, or network configuration not listed in a respective Service Brief.
(ii) Any change to the hardware, software, or network configuration listed in a respective Service Brief.
(iii) Modification of the Customer's application software, hardware or network configuration, including but not limited to installation and configuration of certificates on customer's systems.
(iv) Development of custom solutions including without limitation, scripting and custom dictionaries
(v) Migration of logs or quarantine data from an existing Proofpoint or other vendor's solution.

6. Acceptance of Services

Upon completion of the Services, Proofpoint shall provide written notice (which may be via email) that the Services have been completed. The Services (and associated deliverables) shall be accepted upon completion of the Services by Proofpoint.

7. Fixed Bid Service Fee

The Services described in this Service Brief are delivered during Proofpoint normal business hours (9 AM GMT – 2 AM GMT, Monday – Friday, excluding Proofpoint and local region holidays).

The Services described in this Service Brief are performed on a fixed-price basis at the fees specified in the applicable Proofpoint issued quote for such Services. Such Services are limited to a maximum of twelve (12) consecutive weeks of activity. Interruptions in the Services due to scheduling conflicts by the customer may cause a change in resources and scope as detailed in the Services Scope Changes section above.

The Services will be delivered using Proofpoint's standard delivery model, which may include both onsite and offsite remote delivery of the Services. If the Customer requires a different delivery model (e.g. 100% onsite delivery of Services), the charges, expenses, scope of work and/or schedule are subject to modification in accordance with the Services Scope Changes section above. Unless Customer authorizes such Change Order, Proofpoint and the Customer agree that Proofpoint's standard delivery model will apply for the Services.

8. Invoicing Schedule

Customer will reimburse Proofpoint for the reasonable out-of-pocket expenses incurred in the performance of the Services. Out-of-pocket expenses shall include airfare, lodging, meals, ground transportation as well as all other travel related expenses. Proofpoint will make reasonable efforts to use travel services such as corporate air and hotel rates as requested by Customer. Proofpoint shall obtain Customer's written approval prior to incurring any such expenses. Invoices are issued upon Proofpoint receipt and approval of the Customer's purchase order. Customer authorizes Proofpoint to invoice for, and shall pay additional amounts related to:

(i) Services Scope changes or exceptions.
(ii) Reimbursement of travel related expenses.
(iii) Performance outside Proofpoint normal business hours.