

**HYBRID MEETING OF THE BUSINESS AFFAIRS COMMITTEE
OF THE BOARD OF TRUSTEES
Community College of Philadelphia Wednesday,
May 15, 2024 – 9:00 A.M.**

Present for the Business Affairs Committee: Mr. Michael Soileau, (co-presiding and via zoom), Ms. Mindy Posoff (co-presiding and via zoom), Mr. Jeremiah White (via zoom), Mr. Harold Epps (via zoom), Mr. Rob Dubow (via zoom), and Ms. Dominique Ward (via zoom)

Present for the Administration: Dr. Donald Generals, Dr. Shannon Rooney, Mr. Jacob Eapen, Ms. Jasmine Sessoms (via zoom), Dr. Mellissia Zanjani, Dr. Danielle Liautaud-Watkins, Ms. Carolyn Flynn, Esq., Dr. David Thomas (via zoom), Mr. Derrick Sawyer, Mr. Gim Lim, Mr. John Wiggins, Ms. Marsia Henley, Dr. Darren Lipscomb, Mr. Vijay Sonty, and Mr. Bill Bromley

Guests: Dr. Judith Gay, Vice President Emerita (via zoom), and Ms. Kate McGlinchey, City of Philadelphia (via zoom)

Please see that Attachment A contains a spreadsheet that lists the vendor/consultant, the amount, and the source of funding (i.e. Capital Budget, Operating Budget, Perkins Grant, or Bond Proceeds) which College Administration is seeking approval.

Mr. Soileau called the meeting to order at 9:05 A.M. Mr. Soileau highlighted the agenda items, and asked Mr. Eapen to proceed with item one.

AGENDA
BUSINESS AFFAIRS COMMITTEE
PUBLIC SESSION

(1) Network Assessment and Vulnerability Study (Information Item)

Discussion: Mr. Sonty stated that in January through February of this year we commissioned AccessIT Group to perform an audit of our network and investigate how the network is architected, how devices are connected, how the network is performing, and how safe the network is.

Mr. Sonty also stated that at the completion of the study, a detailed report was presented with details of the potential risks and liabilities discovered within our network (See attachment B). The technical assessment included findings, observations, and recommendations. The goal of this assessment was to provide clear, actionable data about the quality and success of CCP's current security measures. The report offers insights into the potential impact of security threats across the organization, giving the network security team the information needed to manage risks effectively.

The key steps include:

1. Developing a comprehensive asset map
2. Identifying security threats and vulnerabilities
3. Prioritizing risks according to severity

4. Developing security controls in response to risks
5. Documenting the results and creating a remediation plan

The Network Team has successfully mitigated all the critical, high, and medium findings presented in the study.

Mr. Sonty explained the several layers for minimizing security threats and the minimum-security standards of cyber liability.

(2) Construction for Winnet Project (Action Item)

Discussion: Mr. Eapen stated that the Winnet project includes the expansion, renovation and modernization of the existing 8,000 sq. ft. Student Services Space on the Winnet Building first floor to accommodate the needs of KEYS and One Stop programs. The old cafeteria will be designed to accommodate offices for diverse programs and student gatherings. The need met by this project is space for KEYS, Women’s Center, Career Connections, MarcDavid LGBTQ, and the Office of Collegiate Recovery.

Mr. Eapen stated that the College issued RFP #10206 on April 6, 2024 via Penn Bid. The Prebid meeting was held April 12, 2024 and 5 bidders attended. The College received 8 responses. Below are the lowest responsible bidder fees by trade. See Attachment C.

• Torino Construction (General Construction)	\$1,602,660
• Royalty Construction (Fire Protection, HVAC, Plumbing, Electrical)	<u>\$1,302,570</u>
Grand Total:	\$2,905,230

Ms. Henley reported that Torino Construction is 50% female-owned and has six (6) employees, none of whom are minority. Royalty Construction is an MBE firm based out of Pennsauken, NJ and they are 100% minority owned.

In response to Mr. Epps’ questions about the time for bidders to respond to the RFP and distribution, Ms. Henley stated that it was posted on PennBid on April 5, 2024 and the pre-bid was April 12, 2024. Bids were due on April 30, 2024. Mr. Epps commented that the bid response was wide but not deep in diversity of Philadelphia based companies and requested to resume DEI Committee meetings.

Mr. Dubow requested additional information about the split between RACP funding and the Capital Budget.

Recommendation: Staff request that the Business Affairs Committee recommend to the full Board to award Torino Construction (General Construction) in the amount of \$1,602,660, and Royalty Construction (Fire Protection, HVAC, Plumbing, Electrical) in the amount of \$1,302,570 for a total of \$2,905,230. These funds will be paid from RACP funding and the Capital Budget.

Action: Mr. Dubow moved and Mr. White seconded the motion to enter into a contract with Torino Construction for \$1,602,660 and Royalty Construction in the amount of

\$1,302,570 for a grand total of \$2,905,230. The funds from this contract will be from RACP and the Capital Budget. The motion passed unanimously.

(3) Bonnell Skylights (Action Item)

Mr. Eapen stated that staff seeks approval for construction for replacement of the skylight system in Bonnell. The project includes the demolition and installation of a new skylight system over the lobby of Bonnell that connects to the Mint Building. The existing skylight is original to the building, showing signs of age and has reached its useful life. Mr. Soileau asked if it was just one skylight. Mr. Wiggins responded the skylight goes from 16th Street (Mint Building) to 17th Street (Bonnell Building).

The College issued RFP #10205 on May 7, 2024 via Penn Bid. The Pre-bid meeting was held March 28, 2024 and 6 bidders attended. The College received 2 responses. GMI Construction was the lowest bidder. See Attachment D.

Ms. Henley provided demographic information for GMI Construction, and stated that GMI Construction has a total of 25 employees of which 40% are underrepresented minorities.

Staff request that the Business Affairs Committee recommend to the full Board to award GMI Construction in the amount of \$1,191,000 for General Construction. The Bonnell Skylight Project will be paid from RACP funding and the Capital Budget.

Action: Mr. White moved and Mr. Dubow seconded the motion that the Business Affairs Committee recommend to the Board of Trustees to award GMI Construction in the amount of \$1,191,000 for the Bonnell Skylight project. The motion passed unanimously.

NOTE: Ms. Posoff joined the meeting after the action regarding the Bonnell skylights. Mr. Soileau left the meeting after this action, and Ms. Posoff resumed the meeting as Chair.

(4) Grant Thornton (Action Item)

Mr. Eapen stated that in March 2024, Grant Thornton announced that they are partnering with New Mountain Capital, LLC, a New York based investment firm. Angelica Roiz, the partner for Grant Thornton, informed the College that there will be no changes in how they service the College.

New Mountain Capital will allow Grant Thornton to better position the firm to scale and make targeted investments in talent, technology, and infrastructure. The transaction is expected to close before June 30, 2024.

After the closing of the transaction between Grant Thornton and New Mountain Capital, there will be two separate firms. Grant Thornton Advisors LLC will provide business advisory and non-attest services. Grant Thornton LLP, which CCP contracts with, will continue to provide attest (audit) services except they will have a new investor partner, New Mountain Capital. CCP does not have a contract or arrangement with Grant Thornton Advisors for tax services.

The amendment of the term will allow assigning our tax services to their new affiliate, Grant

Thornton Advisors, LLC.

Mr. White asked what happens in 2025 regarding audit services. Mr. Eapen responded that the Audit Committee may recommend a one-year extension or request an RPF. Mr. White asked how many years has CCP been with Grant Thornton? Mr. Gim replied that Grant Thornton has been with CCP for 10 years. Mr. White asked if there will be a change in partners? Mr. Gim replied that Brian Page was the initial partner, and Ms. Angelica Rioz has succeeded Mr. Page.

Staff requests that the Business Affairs Committee recommend to the full Board to approve the Grant Thornton amendments.

Action: Mr. White moved and Mr. Dubow seconded the motion that the Business Affairs Committee recommend to the Board of Trustees to approve the Grant Thornton amendments. The motion passed unanimously.

NOTE: The Business Affairs Committee then briefly recessed the meeting for an Executive Session. The meeting resumed at 10:22am. The Executive Session was to discuss a legal settlement and labor negotiations matters.

Ms. Posoff then requested Ms. Flynn to present the next motions.

(5) Amend Agenda (Action Item)

Ms. Flynn requested that the Committee amends the agenda to include an action item related to a settlement payment to McGoldrick Electric, Inc.

Action: Ms. Ward moved and Ms. Posoff seconded the motion that the Business Affairs Committee amend the agenda as requested. The motion passed unanimously.

(6) McGoldrick Electric Settlement Payments (Action Item)

Staff requested that the Business Affairs Committee recommend to the for Board to approve the settlements payments of \$204,840 for the CATC project and \$202,944 for the Learning & Library Commons project to McGoldrick Electric, Inc.

Action: Ms. Ward moved and Ms. Posoff seconded the motion that the Business Affairs Committee recommend to the Board of Trustees to approve the settlements payments of \$204,840 for the CATC project and \$202,944 for the Learning & Library Commons project to McGoldrick Electric, Inc. The motion passed unanimously.

(7) Next Meeting – Combined Business Affairs and the Board of Trustees (Information Item)

The next combined meeting of the Business Affairs Committee and the Board of Trustees is scheduled for Monday, June 24, 2024 at 9:00 A.M.

Ms. Ward moved to adjourn the Business Affairs Committee meeting and Ms. Posoff seconded that motion. The motion passed unanimously.

JE/tn

c:

Mr. Michael Soileau
Dr. Donald Generals
Mr. Gim Lim
Ms. Marsia Henley
Mr. Derrick Sawyer
Mr. John Wiggins
Ms. Carolyn Flynn, Esq.
Dr. Judith Gay, Vice President Emerita

ATTACHMENT A
FUNDING FOR ACTION ITEMS
MEETING OF THE BUSINESS AFFAIRS
COMMITTEE OF THE BOARD OF TRUSTEES

AGENDA: May 15, 2024

Agenda No.	Vendor/Consultant	Amount	Source
2	Torino Construction	\$1,602,659	Capital Budget & RACP
2	Royalty Construction	\$ 1,302,570	Capital Budget & RACP
3	GMI Construction	\$ 1,191,000	Capital Budget & RACP

ATTACHMENT B

Network Assessment and Vulnerability Study



Network Vulnerability Technical Assessment

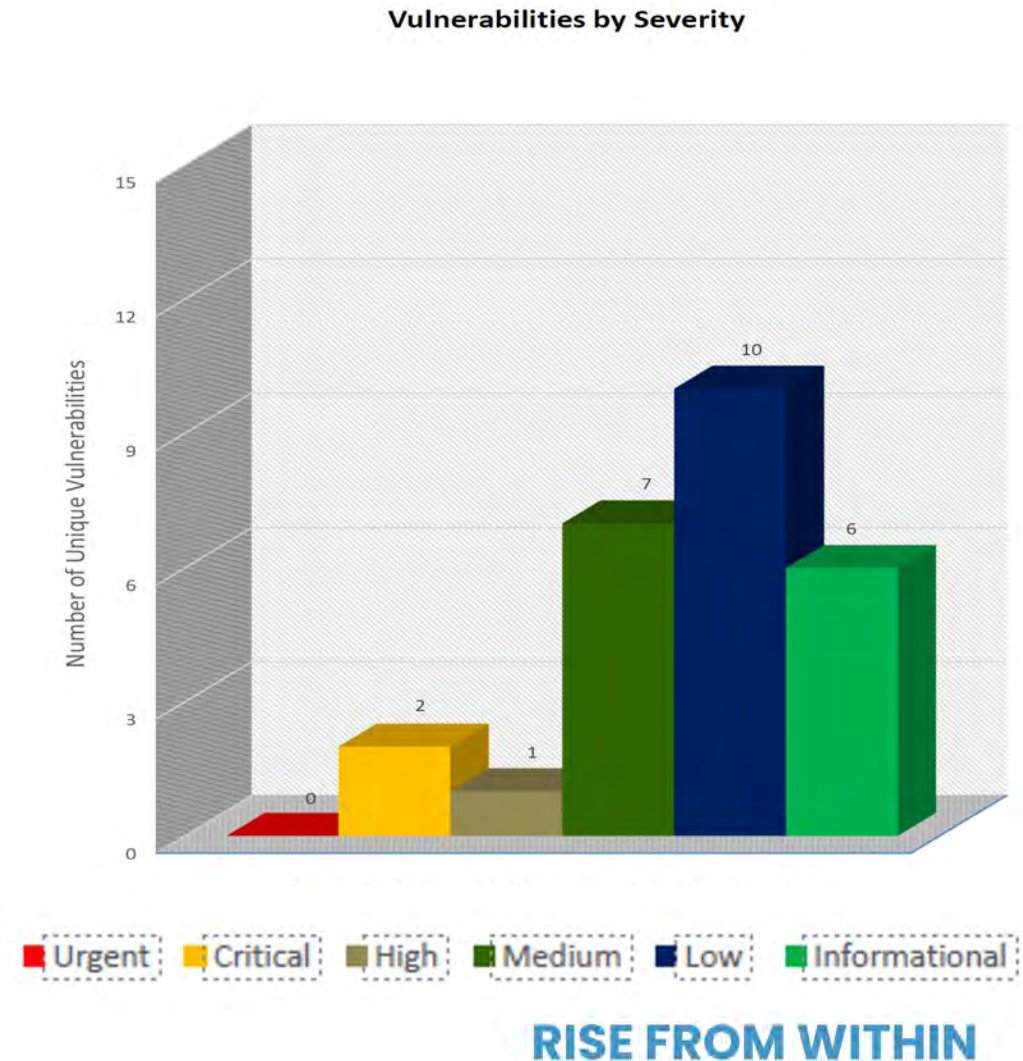
Findings and Remediation Report



External Vulnerability & Penetration Test

Methodology

- Network mapping and reconnaissance
- Identification and validation of vulnerabilities
- Identification of vulnerabilities that could be used to obtain further access





Security Threat Risk Factor Definitions

Urgent Risk – Level 5

Level 5 vulnerabilities provide remote intruders with remote root or remote administrator capabilities. With this level of vulnerability, intruders can compromise the entire host.

Critical Risk – Level 4

Level 4 vulnerabilities give intruders partial access to file-systems (for example, full read access without full write access). Vulnerabilities that expose highly sensitive information also qualify as level 4 vulnerabilities.

High Risk – Level 3

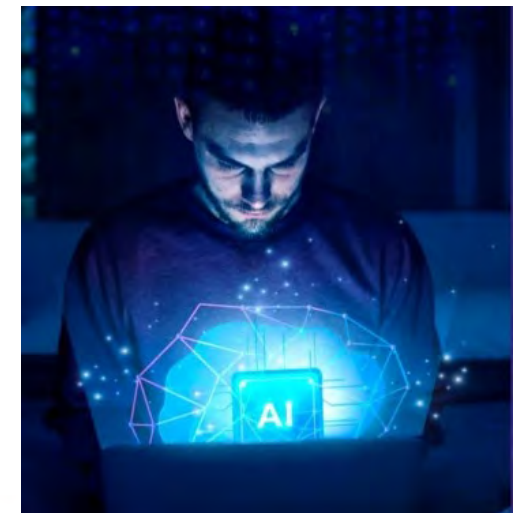
Level 3 vulnerabilities provide intruders with access to specific information stored on the host, including security settings. This level of vulnerability could result in potential misuse of the host by intruders.

Medium Risk- Level 2

Level 2 vulnerabilities expose some sensitive information from the host, such as precise versions of services. With this information, intruders could research potential attacks to try against a host.

Low Risk – Level 1

Level 1 vulnerabilities are those noted which alone have no immediate threat and need to be coupled with other higher severity issues to be part of an actual attack vector.



Task Name	Status	Health	Start Date	End Date	Assigned To	Description/Remediation	% Complete
AccessIT Vulnerability Assessment							
Vulnerability Scan							
CRITICAL findings/Items	Complete		01/04/24	01/15/24			100%
Migrate Listserv Server O/S	Complete		01/04/24	01/15/24	Ferdinand Talabis	Obsolete Version of Microsoft Windows Server 2012	100%
Build new Windows 2022 server VM & Migrate software	Complete		01/04/24	01/15/24	Ferdinand Talabis	Windows2022 Server installed and Listserv software migrated over to new server and tested.	100%
Alertus Application with Default Credentials	Complete		01/04/24	01/15/24	Ed Crosbee	The Alertus Console application is using the default credentials of admin/admin. This would allow anyone to log in to access the application/s and potentially take complete control.	100%
Change Default Credentials In Alertus Application	Complete		01/04/24	01/15/24	Ferdinand Talabis	Changed the default credentials in the Alertus application for the management console..	100%
Set Firewall rule blocking access to management port	Complete		01/04/24	01/15/24	Ed Crosbee	Created a firewall rule on the external firewalls blocking management port access to the Alertus management console.	100%
HIGH findings/Items	Complete		01/04/24	01/15/24	Ed Crosbee		100%
JAMF Server Vulnerabilities:	Complete		01/04/24	01/15/24	Ed Crosbee	Web server vulnerabilities in JAMF application used for managing Mac's.	100%
Browsable Web Directory	Complete		01/04/24	01/15/24	Ferdinand Talabis	Disabled Apache web services on the JAMF server and shutdown the firewall rule allowing server access. JAMF cloud is being used for Mac management now, so server services are obsolete.	100%
Medium findings/Items	Complete		01/04/24				100%
CRC Server Vulnerabilities:	Complete		03/20/24	04/07/24	Joe Polich	IIS web server vulnerabilities in the CRC application.	100%
Microsoft IIS ISAPI Services are Enabled	Complete		03/20/24	04/07/24	Joe Polich	Disabled all unused mappings in IIS. These include the extensions for IDA, IDC, IDQ, HTR, HTW, and PRINTER.	100%
ASP.NET Debug Enabled in IIS	Complete		03/20/24	04/07/24	Joe Polich	Disabled debug mode in IIS for CRC by setting the debug=false in the Web.config file for each application on the IIS server.	100%
ASP.NET Detailed Error Message Information Leak in IIS	Complete		03/20/24	04/07/24	Joe Polich	Disabled detailed ASP.NET error messages by modifying the servers Web.config file. Followed support article http://support.microsoft.com/kb/306355 for detailed instructions.	100%
TLS Server Supports TLS version 1.0 on CRC Server	Complete		03/20/24	04/19/24	Joe Polich	Disable insecure TLS/SSL protocol support in IIS. Configured the web server to require clients to use TLS version 1.2 using Authenticated Encryption with Associated Data (AEAD) capable ciphers. Added - Djdk.tls.client.protocols=TLSv1.2 to the Server Startup.	100%
Faculty Web Server - FTP Supports Clear Text Authentication	Complete		01/04/24	02/01/24	Ed Crosbee	This server is used by several faculty members for uploading syllabus and information for course work. No sensitive information is being transferred, so this is an acceptable risk.	100%
JAMF Server -Potential Apache HTTPD Multiple Vulnerabilities. CVE-2021-39275, CVE-2022-22720,CVE-2022-31813,CVE-2020-11984	Complete		01/04/24	03/19/24	Ferdinand Talabis	Disabled Apache services and shutdown firewall rule which allows remote management access to the server. server access. JAMF cloud is being used for Mac management now, so on-prem services could be disabled.	100%
Comcast Routing Switch Used For Internet Connectivity To FirstLight ISP - Unencrypted Telnet Server is enabled by default.	Complete		02/02/24	02/08/24	Ed Crosbee	Disabled telnet protocol for all VTY lines, and made SSH the default transport protocol for those lines. This is used for remote management access to the switch.	100%
Path Web Server - TLS Server Supports TLS version 1.0	Complete		02/26/24	02/26/24	Ed Crosbee	TLS is used for secure communication between end user devices/applications and web servers. Older versions of TLS (1.0 & 1.1) have vulnerabilities associated with their use and have been disabled on the server..	100%
Labstats Gateway Server - TLS Server Supports TLS version 1.0	Complete		02/26/24	02/26/24	Ed Crosbee	TLS is used for secure communication between end user devices/applications and web servers. Older versions of TLS (1.0 & 1.1) have vulnerabilities associated with their use and have been disabled on the server.	100%
RDP Server - TLS Server Supports TLS version 1.0	Complete		02/26/24	02/26/24	Ed Crosbee	TLS is used for secure communication between end user devices/applications and web servers. Older versions of TLS (1.0 & 1.1) have vulnerabilities associated with their use and have been disabled on the server.	100%
Moveitdmz Server - TLS Server Supports TLS version 1.0	Complete		02/26/24	02/26/24	Ed Crosbee	TLS is used for secure communication between end user devices/applications and web servers. Older versions of TLS (1.0 & 1.1) have vulnerabilities associated with their use and have been disabled on the server.	100%



COMMUNITY COLLEGE OF PHILADELPHIA

Notes & Supplemental Information



RISE FROM WITHIN

STOP



Over the next year there is a

69%
CHANCE
you could be
HACKED!

80% of all cyber crime attacks originate from Russia, China and North Korea

77% of small businesses **don't** regularly back up important data

75% of the health care industry has been infected with malware.*

73% of US citizens have fallen victim to some form of cyber crime

64% of companies have experienced web-based attacks

61% of malicious websites are genuine sites that have been compromised

Social Media Users

50%

Haven't changed their password in the *last year*

20%

Have *never* changed their password

GLOBALLY · COST PER PERSON **6 MONTHS***

\$123

**FIXING
Malware
ATTACKS**

\$441

**LOST
to Cyber
CRIME**

\$271

**PAYING
RANSOMS
to remove malware**

Cyber Liability

Minimum Security Standards

Multi-factor authentication

MFA implemented for all remote access, and also for all access to privileged accounts, even on internal access.

Privileged Access Management (PAM)

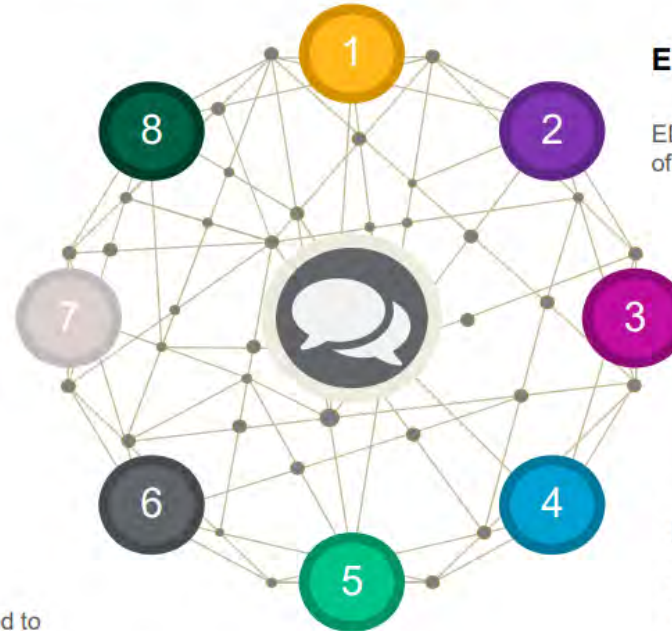
A Privileged Access Management tool in place to manage privileged accounts, and Local Administrative rights granted only on a temporary basis.

Asset Management

Inventory of the environment using a tool for Asset Management.

Segmentation

The environment should be segmented to prevent an attacker from being able to access the entire environment.



Endpoint Detection & Response

EDR rolled out on all servers and endpoints capable of carrying an EDR agent.

Awareness & Phishing training

Awareness training provided to all employees, with phishing simulation campaigns for employees in exposed situations.

Backup procedures

Offline backups or alternative solutions that makes it impossible to delete existing backups.

Active monitoring

The environment must be monitored by a Security Operations Center (SOC), either internal or external, on a 24/7 basis.

Cyber Liability

Minimum Security Standards

MULTIFACTOR AUTHENTICATION (MFA)

Insurers are looking for insureds to utilize MFA to secure:

- Email
- Remote Network Access
- Privileged User Accounts
- Virtual Desktop Instances (VDI)
- Cloud resources including Office365

REMOTE DESKTOP PROTOCOL

RDP is a dominant attack vector for ransomware. Recommendations to secure RDP include:

- VPN
- Encryption
- RDP Gateway
- Complex Passwords
- Multi-Factor Authentication
- Restrict access via a firewall
- Enable Restricted Admin Mode

ADDITIONAL SAFEGUARDS INCLUDE:

- Network Segmentation
- Domain Admin / Service Account management
- PAM (Privileged access management)
- Regular cybersecurity awareness & phishing training
- If using O365, Microsoft Defender for cloud-based protections
- Minimize the number of Local Administrator Accounts & ensure each is unique
- Patching cadence / policy
- End-point detection and response (EDR) practices
- SIEM – event monitoring and log management

BACK-UP POLICIES

Properly secured back-ups reduce the severity of Ransomware losses. Recommendations include:

- Encrypting backups
- Segregating backups; physically stored offsite and offline, immutability
- Regularly performing full and incremental backups of data
- Regular testing of backups for data integrity and restorability
- Annual testing of Business Continuity / Disaster Recovery / Incident Response Plans



Cloud



Apps



Email



Endpoint



Network



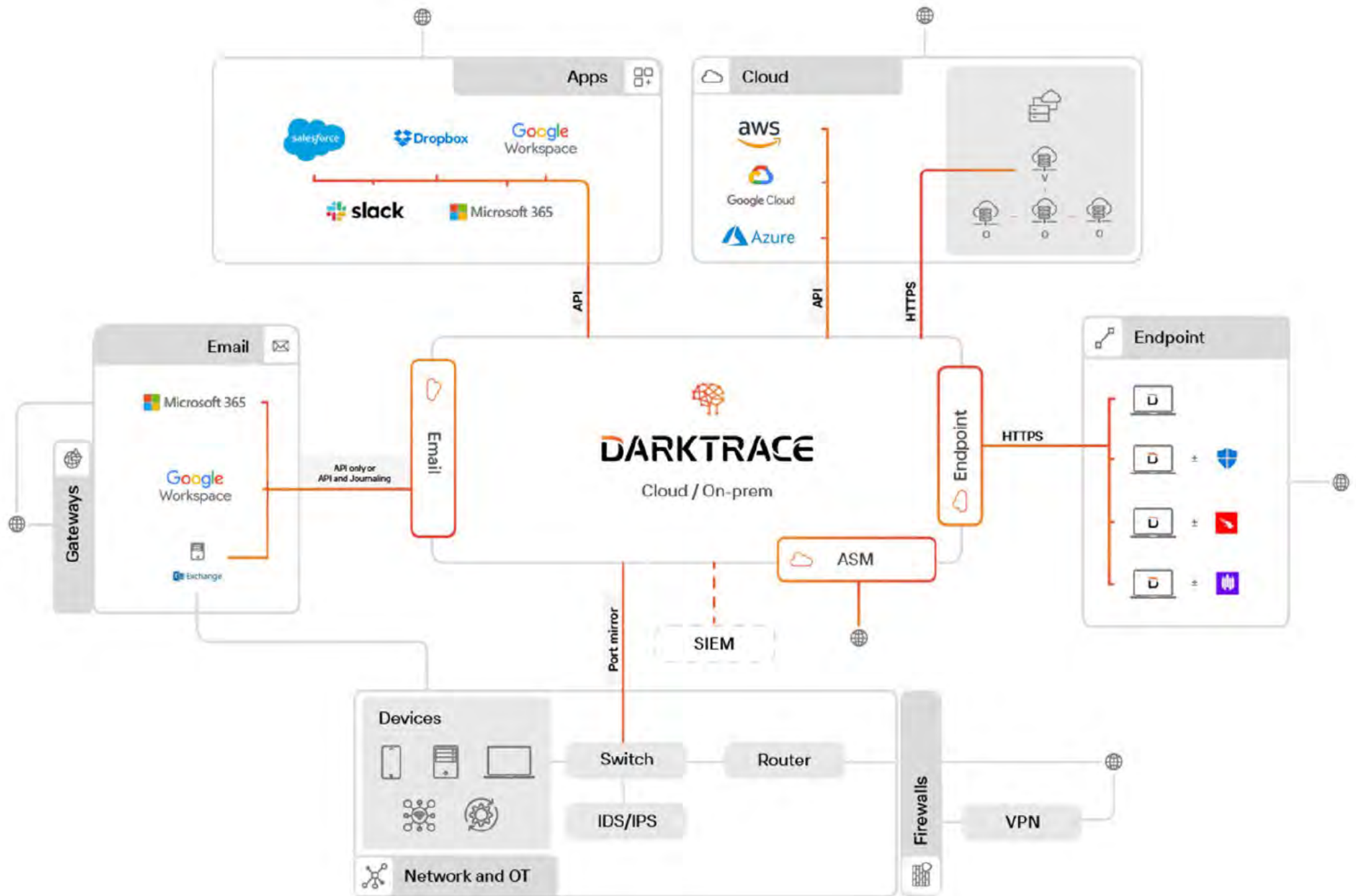
Zero Trust

Organizations now need to
continuously and *consistently*
validate/act on their Cyber
Security Risks

Validate

Remediate

Repeat





COMMUNITY COLLEGE OF PHILADELPHIA



RISE FROM WITHIN

ATTACHMENT C

Construction for Winnet Project Bids

	TORRADO	BEDWELL	EPGUIDI	JJB	HYDE	TORINO	ROYALTY	SMITH
Status	Total Cost	Total Cost	Total Cost	Total Cost	Total Cost	Total Cost	Total Cost	Total Cost
General Construction								
Basket Total	\$ 1,998,400.00	\$ 2,342,479.00	\$ 1,687,539.00	\$ -	\$ -	\$ 1,602,659.00	\$ -	\$ 1,818,000.00
Fire Protection								
Basket Total	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ 78,625.00	\$ -
Plumbing Construction								
Basket Total	\$ -	\$ -	\$ -	\$ 222,000.00	\$ -	\$ -	\$ 174,001.00	\$ -
HVAC Construction								
Basket Total	\$ -	\$ -	\$ -	\$ 396,000.00	\$ -	\$ -	\$ 173,897.00	\$ -
Electrical Construction								
Basket Total	\$ -	\$ -	\$ -	\$ -	\$ 1,276,600.00	\$ -	\$ 876,047.00	\$ -
Grand Total	\$ 1,998,400.00	\$ 2,342,479.00	\$ 1,687,539.00	\$ 618,000.00	\$ 1,276,600.00	\$ 1,602,659.00	\$ 1,302,570.00	\$ 1,818,000.00

ATTACHMENT D

Bonnell Skylights Bids

				GMI		Crystal Structures	
Status	Description	Unit of Measure	Quantity Required	Unit Price	Total Cost	Unit Price	Total Cost
Base Bid Pricing							
Success: All values provided	General Requirements (Other)	LS	1	\$ 0.00	\$ 0.00	\$ -	\$ -
Success: All values provided	Contractors Contingency	LS	1	\$ 0.00	\$ 0.00	\$ -	\$ -
Success: All values provided	Permits and Inspection Fees	LS	1	\$ 0.00	\$ 0.00	\$ -	\$ -
Success: All values provided	Insurance	LS	1	\$ 23,820.00	\$ 23,820.00	\$ -	\$ -
Success: All values provided	General Contractor's Fee (OH+P)	LS	1	\$ 0.00	\$ 0.00	\$ -	\$ -
Success: All values provided	Atrium Cleaning	LS	1	\$ 10,000.00	\$ 10,000.00	\$ -	\$ -
Success: All values provided	Selective Demolition	LS	1	\$ 86,932.00	\$ 86,932.00	\$ -	\$ -
Success: All values provided	Metals	LS	1	\$ 15,000.00	\$ 15,000.00	\$ -	\$ -
Success: All values provided	Wood and Plastics	LS	1	\$ 0.00	\$ 0.00	\$ -	\$ -
Success: All values provided	Thermal and Moisture Protection	LS	1	\$ 12,200.00	\$ 12,200.00	\$ -	\$ -
Success: All values provided	Metal Framed Skylights	LS	1	\$ 1,043,048.00	\$ 1,043,048.00	\$ 258,900.00	\$ 258,900.00
Success: All values provided	Glazing	LS	1	\$ 0.00	\$ 0.00	\$ -	\$ -
Basket Total					\$ 1,191,000.00		\$ 258,900.00
Grand Total					\$ 1,191,000.00		\$ 258,900.00

*Crystal Structures did not submit the required documentation or give