RE: Meeting follow up

Wutoh, Anthony <awutoh@Howard.edu>
Fri 2/25/2022 9:33 AM

To: Alfred, Marcus <marAlfred@Howard.edu>;Osaghae, Olga <olga.osaghae@howard.edu>;Ankoni Lowman <alowman@gocloudforce.com>
Cc: Dubroy, Tashni-Ann <tashni.dubroy@Howard.edu>;Cue, Jahmal <jahmal.cue@Howard.edu>;Frederick, Wayne <HUPresident@Howard.edu>;Royal, Guericke <groyal@Howard.edu>;Larry Morse <lcmorse@fairviewcapital.com>;Wingate, La'Marcus <lamarcus.wingate@howard.edu>;Jones, Bruce <bruce.jones@Howard.edu>;Taylor, Christie <christie.taylor@Howard.edu>;Patterson, Rubin <rubin.patterson@howard.edu>

Dr. Alfred,

Good morning, your request for an independent ISP/external network connection has been thoroughly reviewed by ETS, and expert consultants supporting the University. As has been stated previously, your request is denied, and will not be considered any further for security reasons outlined extensively. Thank you.

AKW

Anthony K. Wutoh, Ph.D., R.Ph.
Provost & Chief Academic Officer
Howard University | 2400 6th St. NW, Suite 306 | Washington DC, 20059
Desk: 202.806.2550| awutoh@howard.edu
"Excellence in Truth and Service"

From: Alfred, Marcus <marAlfred@Howard.edu>
Sent: Thursday, February 24, 2022 3:56 PM
To: Osaghae, Olga <olga.osaghae@howard.edu>; Ankoni Lowman <alowman@gocloudforce.com>
Cc: Dubroy, Tashni-Ann <tashni.dubroy@Howard.edu>; Cue, Jahmal <jahmal.cue@Howard.edu>; Wutoh, Anthony <awutoh@Howard.edu>; Frederick, Wayne <HUPresident@Howard.edu>; Royal, Guericke <groyal@Howard.edu>; Larry Morse <lcmorse@fairviewcapital.com>; Wingate, La'Marcus <lamarcus.wingate@howard.edu>; Jones, Bruce <bruce.jones@Howard.edu>; Taylor, Christie <christie.taylor@Howard.edu>
Subject: Re: Meeting follow up

Good afternoon,

Just following up on this. We are ordering a high performance compute server as well as hoping to plan to order networking equipment to upgrade the computational physics lab. Again, the Navy gave us funding to do this. If ETS won't allow us access and the HU administrative leadership won't step in to make this right, I need to let the Navy know.

Again, I've shown the security argument maintained by ETS doesn't apply - a separate connection can't take down the HU main campus network. I've also shown that ETS should probably talk a bit more with myself and other researchers about our research requirements.

Finally, past faculty, administrators, and board members agreed that HU faculty should be consulted before policies are created or changed that affect academics for good reasons. One reason seems to have been to avoid this kind of issue that can bring some research to a standstill and make HU less competitive.

Thank you,

Marcus Alfred
Pronouns: he, him, his
Associate Professor
Howard University
Dept. of Physics & Astronomy
Washington, DC 20059
202-806-6258
maralfred@howard.edu

From: Alfred, Marcus <marAlfred@Howard.edu>
Sent: Thursday, February 17, 2022 12:40 PM
To: Osaghae, Olga <olga.osaghae@howard.edu>; Ankoni Lowman <alowman@gocloudforce.com>
Cc: Dubroy, Tashni-Ann <tashni.dubroy@Howard.edu>; Cue, Jahmal <jahmal.cue@Howard.edu>; Wutoh, Anthony <awutoh@Howard.edu>; Frederick, Wayne <HUPresident@Howard.edu>; Royal, Guericke <groyal@Howard.edu>; Larry Morse <lcmorse@fairviewcapital.com>; Wingate, La'Marcus <lamarcus.wingate@howard.edu>; Jones, Bruce <bruce.jones@Howard.edu>; Taylor, Christie <christie.taylor@Howard.edu>
Subject: Re: Meeting follow up

Good morning CIO Osaghae,

I'm just following up on my questions. If an external connection and network can't take the HU campus network down (no impact on HU's campus network), as it seems to be the case from my previous email, and it's not costing the HU administration anything, why not explore this option?

Especially since this external connection does seem to satisfy my group's research and teaching needs.

Thank you,

Marcus Alfred
Pronouns: he, him, his
Associate Professor
Howard University
Dept. of Physics & Astronomy
Washington, DC 20059
202-806-6258
maralfred@howard.edu

From: Alfred, Marcus <marAlfred@Howard.edu>
Sent: Wednesday, February 16, 2022 12:22 PM
To: Osaghae, Olga <olga.osaghae@howard.edu>; Ankoni Lowman <alowman@gocloudforce.com>
Cc: Dubroy, Tashni-Ann <tashni.dubroy@Howard.edu>; Cue, Jahmal <jahmal.cue@Howard.edu>; Wutoh, Anthony <awutoh@Howard.edu>; Frederick, Wayne <HUPresident@Howard.edu>; Royal, Guericke <groyal@Howard.edu>; Larry Morse <lcmorse@fairviewcapital.com>; Wingate, La'Marcus <lamarcus.wingate@howard.edu>; Jones, Bruce <bruce.jones@Howard.edu>
Subject: Re: Meeting follow up

Dear CIO Osaghae,

Again, you haven't - please take a look at the questions again and a closer look at your responses.

1. How would having our own separate connection and network bring down HU's network? An analogy is how would my home network take down HU's campus network if i cannot connect to HU's network from my home?
2. How can you exceed my requirements when you barely know anything about them?

For (1) your response was:

New attack surface that belongs to Howard University

- New public IP with an ISP that has not been approved
- IP's not being scanned regularly for port\security compliance

->How does this bring down the HU Network? Even if this were true (which it isn't) this only impacts our internal network, not the HU campus network.

- You would be introducing a new threat attack surface for Howard University Data
  - Data can be ingressed and egressed with no protection

->How does this bring down the HU network? This would be internal data to our lab and nothing else on campus. Our work is academic and would be public (not classified or owned by the government).

- You would be introducing non hardened or secure workstations and servers
  - No STIG\GPOs
  - No central HIPS\HIDS\AV solution

-> How does this bring down the HU network? Again, our new connection would be physically separate from the HU network. So even if we had a microsoft environment without antivirus or any intrusion detection or any security guidelines (which isn't true and another bad assumption), we still aren't connected to HU's campus

network. Again, the analogy I made earlier still applies - how can a random residential home network in (for example) Richmond VA take down HU's campus network?

- You will be creating a decentralized network meaning that overlapping could exist
  - This could cause networking issues.

-> How does this bring down the HU network? How can they overlap? They are physically distinct. How can the residential network in Richmond VA overlap with HU?

- Your ISP has no perimeter defense
  - No Intrusions Detection Systems (IPS)\ Intrusion Protection System (IDS) functionality to block from attacks.

-> How does this bring down the HU network? Same problem as mentioned above. (Assuming we would have zero security - which is not true) If this separate network is not connected to HU's campus network how can this take down HU's campus network? Again, if a residential home network in Richmond VA has no security and is compromised, how doe that bring down HU's campus network?

- Lack of network monitoring
  - No ability to detect an intrusion that is propagating or moving laterally

-> How does this bring down the HU campus network? Assuming we wouldn't monitor our network (again an incorrect assumption), our network would be physically separate from the campus network. There would be zero trust between our network and the HU campus network - no more than any other network in the world. If a random residential network in Richmond can't take down HU's campus network, how could our proposed network do so?

I hope this is clear. The answers you provided say absolutely nothing about how our proposed external connection could take down HU's campus network. Please don't presume we are completely clueless.

Any policy change that has an impact on academics is supposed to also be considered by the senate. This is in HU Board of Trustee approved documents and unfortunately not followed nearly enough.

Thank you,

Marcus Alfred
Pronouns: he, him, his
Associate Professor
Howard University
Dept. of Physics & Astronomy
Washington, DC 20059
202-806-6258
maralfred@howard.edu

From: Osaghae, Olga <olga.osaghae@howard.edu>
Sent: Wednesday, February 16, 2022 11:28 AM
To: Alfred, Marcus <marAlfred@Howard.edu>; Ankoni Lowman <alowman@gocloudforce.com>
Cc: Dubroy, Tashni-Ann <tashni.dubroy@Howard.edu>; Cue, Jahmal <jahmal.cue@Howard.edu>; Wutoh, Anthony <awutoh@Howard.edu>; Frederick, Wayne <HUPresident@Howard.edu>; Royal, Guericke <groyal@Howard.edu>; Larry Morse <lcmorse@fairviewcapital.com>; Wingate, La'Marcus <lamarcus.wingate@howard.edu>; Jones, Bruce <bruce.jones@Howard.edu>
Subject: RE: Meeting follow up

Good morning, Dr. Alfred –

We have not dismissed your concerns/questions but have answered and explained exhaustively below.

With regards to Policy that should have said "Howard University **ETS** Policies and Procedures" as these are departmental/unit policies and procedures to secure our Cybersecurity posture.

Best Regards,

Olga Osaghae MS, PMP| Interim Chief Information Officer
Enterprise Technology Services | Wonder Plaza, Technology Center
Email: olga.osaghae@howard.edu | Office: 202-806-0897 | Cell: 202-368-7021

From: Alfred, Marcus <marAlfred@Howard.edu>
Sent: Wednesday, February 16, 2022 10:59 AM
To: Ankoni Lowman <alowman@gocloudforce.com>; Osaghae, Olga <olga.osaghae@howard.edu>
Cc: Dubroy, Tashni-Ann <tashni.dubroy@Howard.edu>; Cue, Jahmal <jahmal.cue@Howard.edu>; Wutoh, Anthony <awutoh@Howard.edu>; Frederick, Wayne <HUPresident@Howard.edu>; Royal, Guericke <groyal@Howard.edu>; Larry Morse <lcmorse@fairviewcapital.com>; Wingate, La'Marcus <lamarcus.wingate@howard.edu>; Jones, Bruce <bruce.jones@Howard.edu>
Subject: Re: Meeting follow up

Good morning CIO Osaghae,

I'll continue to address my emails to you since this is supposed to be a discussion with the HU Administrative leadership.

If there is an aim to be constructive and positive, please stop making disparaging assumptions about our lab that are not true. We've had to endure these types of insults with grant proposals and other research work for a long time. There've been assumptions that HBCU faculty and African American faculty in particular, can't deliver on research and maintain a workable infrastructure.

For decades our lab has survived, functioned, produced research products, and remained secure with almost no support or security from the HU administration. We've produced faculty, PhD's, and graduates that have gone on to successful careers around the country. We currently have one of the largest awards on campus and before the workday implementation funded over 12 students and we currently fund over 10 postdocs and research scientists. Our lab is on track to become the largest producer of African American astrophysicsts in the world.

So would you and your team please stop dismissing my concerns and questions, and answer them directly.

1. How would having our own separate connection and network bring down HU's network? An analogy is how would my home network take down HU's campus network if i cannot connect to HU's network from my home?
2. How can you exceed my requirements when you barely know anything about them?
3.

I look forward to a discussion with HU's Administration and Board leadership to address this issue and correct the lapse in adhering to HU Board approved policy by making academic (research) policy decisions without involving faculty through the HU Faculty Senate.

Thank you,

Marcus Alfred
Pronouns: he, him, his
Associate Professor
Howard University
Dept. of Physics & Astronomy
Washington, DC 20059
202-806-6258
maralfred@howard.edu

From: Ankoni Lowman <alowman@gocloudforce.com>
Sent: Tuesday, February 15, 2022 11:16 PM
To: Alfred, Marcus <marAlfred@Howard.edu>; Osaghae, Olga <olga.osaghae@howard.edu>
Cc: Dubroy, Tashni-Ann <tashni.dubroy@Howard.edu>; Cue, Jahmal <jahmal.cue@Howard.edu>; Wutoh, Anthony <awutoh@Howard.edu>; Frederick, Wayne <HUPresident@Howard.edu>; Royal, Guericke <groyal@Howard.edu>; Larry Morse <lcmorse@fairviewcapital.com>; Wingate, La'Marcus <lamarcus.wingate@howard.edu>
Subject: RE: Meeting follow up

Hi Marcus,

I would like to keep the tone of these emails positive and constructive. I'm noticing that your emails are saying item such as "do you even know", statement like this can be hurtful. I am not questioning you or your intelligence, I am however advising you and my leadership on the cyber impact of doing something like this. That being said, I have included responses below:

I noticed that you are very focused on networking. There are many parts of Cyber such as data, users, devices, etc, with networking being an aspect of it. Cyber is much larger than simple an ISP you wish to bring in, but there is the data you plan to hold, the people that deal with the data, how the data is sent, how its received, how we meet compliance, how we protect ourselves from threats and more.

I'd like to clarify that you did not ask that question. You asked:
"As i asked in the meeting today and in emails before, if I get a physically independent external connection and network in my lab, how would that impact the HU network security in any way? They would be completely separate."

We had the following response to your inquiry:

There are several impacts when pulling a new network which impacts the overall infrastructure as the data\hardware\intellectual property belongs to the University. Here are just a couple:

- New attack surface that belongs to Howard University
  - New public IP with an ISP that has not been approved
  - IP's not being scanned regularly for port\security compliance
- You would be introducing a new threat attack surface for Howard University Data
  - Data can be ingressed and egressed with no protection
- You would be introducing non hardened or secure workstations and servers
  - No STIG\GPOs
  - No central HIPS\HIDS\AV solution
- You will be creating a decentralized network meaning that overlapping could exist
  - This could cause networking issues.
- Your ISP has no perimeter defense
  - No Intrusions Detection Systems (IPS)\ Intrusion Protection System (IDS) functionality to block from attacks.
- Lack of network monitoring
  - No ability to detect an intrusion that is propagating or moving laterally

As a note to your statement:

> "(And by the way, the Navy seems to be fine with our proposal and has added no security restrictions. Zero. But we are fully funded.)"

Not knowing about documents such NIST 800 171 (attached) like this is why Security SME's like myself are here to help. Federal compliance or governance around Federal data is an important topic. Severe legal lawsuits can\have happened when government material isn't properly store and\or handled. I would recommend reading through the attached documentation, as it contains great information in details in this regards.

Your statement around:

> "In your email you said,
> - Your system gets infected with a virus\trojan\ransomware
>   - There is nothing stopping it from propagating further to others."

This is mainly talking about lateral propagation across your lab. The way attackers operated is different than many think, usually steal data, compromise user accounts, then when they don't need to take anything else, initiate the attack. and users accounts. In Cyber, users are just as vulnerable to attack as devices are, events such as credential harvesting.

In regards to the requirements. You provided several requirements in your initial email and we exceeded all of them.

I'd like to notate that we have been trying to protect the University cyber posture, while working with departments to fulfil their needs, to this point, everyone has not only been taken care of, but has seen increased performance, better agility, better cost effectiveness, all while increasing and abiding by our security. Allowing a lab infrastructure with no governance, no security policies, no management, no visibility, utilizing government and University sensitive data goes against every rule in cyber security.

Thanks,

Ankoni Lowman

From: Alfred, Marcus <marAlfred@Howard.edu>
Sent: Tuesday, February 15, 2022 22:23
To: Osaghae, Olga <olga.osaghae@howard.edu>
Cc: Dubroy, Tashni-Ann <tashni.dubroy@Howard.edu>; Cue, Jahmal <jahmal.cue@Howard.edu>; Ankoni Lowman <alowman@gocloudforce.com>; Wutoh, Anthony <awutoh@Howard.edu>; Frederick, Wayne <HUPresident@Howard.edu>; Royal, Guericke <groyal@Howard.edu>; Larry Morse <lcmorse@fairviewcapital.com>; Wingate, La'Marcus <lamarcus.wingate@howard.edu>
Subject: Re: Meeting follow up

Good evening CIO Osaghae,

Thank you for your email. But you still did not answer my question. How would having our own separate connection bring down HU's network? (And by the way, the Navy seems to be fine with our proposal and has added no security restrictions. Zero. But we are fully funded.)

In your email you said,

- Your system gets infected with a virus\trojan\ransomware
  - There is nothing stopping it from propagating further to others.

How is this possible if our network will be completely separate from the HU network? And I'm asking again, how would having our own separate connection and network bring down HU's network?

Also, you mentioned the following,

"During our previous sessions, we provided a solution that not only met your requirements but exceeded them. In addition, the solution, met the requirements of the university. We would love the chance to hear why it would not be a viable solution."

If you met my requirements then do you know the proprietary software we will run? Or do you know anything about the custom NASA software one of our users runs that's very environment dependent ? Have we even started talking about the satellite data link for a funded ground station? Do you know what our teaching and training needs are for the next generation of African American computational physicists?

How can you exceed my requirements when you barely know anything about them?

I'm concerned that you aren't answering a pretty straight forward question and more concerned now that I realize academic (research) policy has been made without any HU Faculty Senate input contrary to HU Board approved documents.

Sincerely,

Marcus Alfred
Pronouns: he, him, his
Associate Professor
Howard University
Dept. of Physics & Astronomy
Washington, DC 20059
202-806-6258
maralfred@howard.edu

From: Osaghae, Olga <olga.osaghae@howard.edu>
Sent: Tuesday, February 15, 2022 8:54 PM
To: Alfred, Marcus <marAlfred@Howard.edu>
Cc: Dubroy, Tashni-Ann <tashni.dubroy@Howard.edu>; Cue, Jahmal <jahmal.cue@Howard.edu>; Ankoni Lowman <alowman@gocloudforce.com>; Wutoh, Anthony <awutoh@Howard.edu>; Frederick, Wayne <HUPresident@Howard.edu>; Royal, Guericke <groyal@Howard.edu>; Larry Morse <lcmorse@fairviewcapital.com>
Subject: RE: Meeting follow up

Good evening, Dr. Alfred –

Thank you for your response. I understand you will like your own ISP but as we have stated several times there are security implications. Since the ransomware attack, ETS and the Cyber Security Team have been working tirelessly to secure the University and build back a better infrastructure. The entire team came together to respond to your email below and it covers 3 areas:

- Howard University Cyber Strategy
- Howard University Data and Property
- Howard University ETS Procedures

As Howard University continues to improve its cyber security posture, we are implementing cyber security controls across the University. We are consolidating, centralizing, and creating services for the entire University to consume including research and development infrastructure. As I am sure you are aware, the security of the University is paramount. We have implemented multi factor authentication, endpoint security monitoring, vulnerability scanning, pen testing, security hardening guidelines, and logging monitoring just to name a few. Hence, it is critical that anything we do calls for a more secure path to ensure that our university is safe.

As it pertains to the data, hardware, internet lines, closets, server, wall jacks, buildings, DMARC, wires in the wall, those all belong to Howard University, specifically the responsibility belongs to ETS. Even if your system exists on a separate network, we are still responsible for the data, compliance, access, authorization and more because at the end of the day even if a security issue occurs in a department is still a university security issue.

There are also several compliance matrices we must meet as an organization in order to reduce our attack surface and ensure we have consistent security across the board. Leadership decisions have been made to standardize IT\security across the University such as College of Dentistry, Researcher-Sickle Cell, Researchers-Ansys, Contractor Teams just to name a few. This in turn helps when we conduct our cyber security posture assessment and when auditors come in to assess the environment for vulnerability. Please see attached for NIST SP 171 – Protecting Controlled Unclassified Information in Nonfederal Systems and Organization. If you plan on housing government data as stated in your email, then you will have to comply with this document. Based on the control sets in the document such as AC and CP, you will not be able to pass NIST standards.

There are several impacts when pulling a new network which impacts the overall infrastructure as the data\hardware\intellectual property belongs to the University. Here are just a couple:

- New attack surface that belongs to Howard University
  - New public IP with an ISP that has not been approved
  - IP's not being scanned regularly for port\security compliance
- You would be introducing a new threat attack surface for Howard University Data
  - Data can be ingressed and egressed with no protection
- You would be introducing non hardened or secure workstations and servers
  - No STIG\GPOs
  - No central HIPS\HIDS\AV solution
- You will be creating a decentralized network meaning that overlapping could exist
  - This could cause networking issues.
- Your ISP has no perimeter defense
  - No Intrusions Detection Systems (IPS)\ Intrusion Protection System (IDS) functionality to block from attacks.
- Lack of network monitoring
  - No ability to detect an intrusion that is propagating or moving laterally

Use case breaches just to name a couple:

- If a user in your lab connects to a website and downloads a piece of software that contains malware then the malware pulls data out of the organization
  - This is a breach of data within the University's policy
- If a user's password is compromised and another non-authorized individual logs in and takes data
  - This is cyber security incident of unauthorized access.
- If a user leaves a computer unattended and another visitor walks in a uses the computer and takes data due to no lock out policy
  - This is cyber security incident of unauthorized access.
- Your connection gets breached using a Man In The Middle (MITM)
  - Your system has no IDS\IPS \Audit Logging where you could even see if this happened.
- Your system gets DDoS
  - You have no system to detect this where you could even see if this happened.
- Your system gets infected with a virus\trojan\ransomware
  - There is nothing stopping it from propagating further to others.

Your isolated system lacks the following, which deems it not secure enough to operate in the Howard University environment: Just to name a few below.

- Access Control Plane
  - No logging of who\what\where when people have logged in
  - No central identity management
- Computer
  - Endpoint Security and Detection
    - No HIPS\HIDS\AV mandate can cause a massive security vulnerability where data and users can be compromised.
  - No configuration management\hardening or STIGing
    - No configuration management, GPO hardening or standardizing of the workstation also for massive holes in security, items like SMBv1, outdated TLS\SSL protocols, or other vulnerable items can be exploited fairly easily
- SEIM Logging
  - No centralized logging or AI reviewing logs
- Physical Security
  - No central physical security in place
- User Access Security
  - Password expiration
  - Two factor authentication
  - Segregation of user accounts
  - User Onboard and User Offboard
- Howard University Policies and Procedures
  - Rules of Behavior
  - Acceptable Use Policy
- Data Protection
  - Data Encryption
    - Laptop\workstation encryption
  - Data in Transit
    - SSL data encryption.

Your statement of the following does not reflect accurately.

"We'd like to continue doing this without being forced into a particular vendor's solution or shutting down our lab. Which it appears is what the lab is facing now."

Your department is being asked to conform with security policies and utilize the secure solutions developed by ETS and the Cyber security team. As we have shown and demonstrated to you already, we have a fully operational Cloud environment which other colleges and researchers are already using. We have also mentioned to you we are happy to talk through other options which would have included an external colocation if you choose to maintain the use of physical servers to ensure your department and researchers can continue to operate in an efficient manner. During our previous sessions, we provided a solution that not only met your requirements but exceeded them. In addition, the solution, met the requirements of the university. We would love the chance to hear why it would not be a viable solution.

As always, the ETS Team is willing and ready to help. It is not our intent to impede work as when Howard moves forward, our entire community (students, faculty, and staff) all benefit. However, the safety and security of the University comes first. The desire to push forward to have your own ISP and not understand our cyber security posture only puts your department and the University at risk.

We will be on standby when you are ready to discuss other paths forward.

Best Regards,

Olga Osaghae MS, PMP| Interim Chief Information Officer
Enterprise Technology Services | Wonder Plaza, Technology Center
Email: olga.osaghae@howard.edu | Office: 202-806-0897 | Cell: 202-368-7021

From: Alfred, Marcus <marAlfred@Howard.edu>
Sent: Tuesday, February 15, 2022 5:33 PM
To: Osaghae, Olga <olga.osaghae@howard.edu>
Cc: Dubroy, Tashni-Ann <tashni.dubroy@Howard.edu>; Cue, Jahmal <jahmal.cue@Howard.edu>; Ankoni Lowman <alowman@gocloudforce.com>; Wutoh, Anthony <awutoh@Howard.edu>; Frederick, Wayne <HUPresident@Howard.edu>; Royal, Guericke <groyal@Howard.edu>; Larry Morse

<lcmorse@fairviewcapital.com>
Subject: Re: Meeting follow up

Good afternoon,

I look forward to the next meeting with Dr. Dubroy or any other administrators. As i asked in the meeting today and in emails before, if I get a physically independent external connection and network in my lab, how would that impact the HU network security in any way? They would be completely separate.

I still didn't get a good answer to that question. The response in our meeting today of "someone might plug somethng into the wrong port" doesn't make any kind of sense to me.

Given that we've had zero major security intrusions for over 30 years in the computational physics lab and the ETS ransomware attack had no impact on any of our systems, catastrophic security failures aren't things we are prone to in the lab.

We've trained Black and African American network engineers, software engineers, and computational scientists that write custom codes for both theoretical and experimental published work. We'd like to continue doing this without being forced into a particular vendor's solution or shutting down our lab. Which it appears is what the lab is facing now.

The Navy trusted us with funding (about a million dollars) for a computational project and rebuilding our networking and computational capacity. It would be great if the HU administration not impede us from exploring options (that have apparently zero security impacts on the HU network) to do this work.

Thank you,

Marcus Alfred
Pronouns: he, him, his
Associate Professor
Howard University
Dept. of Physics & Astronomy
Washington, DC 20059
202-806-6258
maralfred@howard.edu

From: Osaghae, Olga <olga.osaghae@howard.edu>
Sent: Tuesday, February 8, 2022 12:13 PM
To: Alfred, Marcus <marAlfred@Howard.edu>
Cc: Dubroy, Tashni-Ann <tashni.dubroy@Howard.edu>
Subject: RE: Meeting follow up

Good afternoon, Dr. Alfred –

I understand your concerns. Your decision calls for a bigger conversation especially where Security is concerned as outlined below and until we iron that out to include mitigation, I cannot support this.
ETS team (Networking, Security and SysOps) will be available to meet so we all understand the impact of this decision.

Best Regards,

Olga Osaghae MS, PMP| Interim Chief Information Officer
Enterprise Technology Services | Wonder Plaza, Technology Center
Email: olga.osaghae@howard.edu | Office: 202-806-0897 | Cell: 202-368-7021

From: Alfred, Marcus <marAlfred@Howard.edu>
Sent: Tuesday, February 8, 2022 11:40 AM
To: Osaghae, Olga <olga.osaghae@howard.edu>; alowman@gocloudforce.gom
Subject: Fw: Meeting follow up

Marcus Alfred
Pronouns: he, him, his
Associate Professor
Howard University
Dept. of Physics & Astronomy
Washington, DC 20059
202-806-6258
maralfred@howard.edu

From: Alfred, Marcus <marAlfred@Howard.edu>
Sent: Tuesday, February 8, 2022 7:43 AM
To: Ankoni Lowman <alowman@gocloudforce.com>
Subject: Re: Meeting follow up

Hi VP Osaghae and Dr. Lowman,

Thank you for the response, I understand that the external connection will not be connected to HU's internal network. That's fine. We've made our decision.

We'll go ahead and make arrangements for an external network connection with a different ISP.

We'd appreciate the CIO's office support in making this as painless as possible.

Thanks again,

Marcus

Marcus Alfred
Pronouns: he, him, his
Associate Professor
Howard University
Dept. of Physics & Astronomy
Washington, DC 20059
202-806-6258
maralfred@howard.edu

From: Ankoni Lowman <alowman@gocloudforce.com>
Sent: Monday, February 7, 2022 4:26 PM
To: Alfred, Marcus <marAlfred@Howard.edu>; Osaghae, Olga <olga.osaghae@howard.edu>
Subject: RE: Meeting follow up

Hi Marcus –

Thanks for reaching out. There are many security and core issues with pulling a 3rd party ISP. There is no DMARC, networking backbone for them to come into, there is no centralized routing, and there's no centralized protection. For this to occur you'd have constructions costs, telco closet re-wires, and more. I would estimate three to six months of work, and construction cost without any layer 2 or layer 3 configurations to be 5k depending on the ISP that you choose. I think in total, time, constructions + labor would be in the 10k – 15k range for everything.

Additionally, if you choose to go with another ISP we cannot connect to it from Azure as there will be no central routing available since it is isolated. I'm happy to jump on another call and walk through the issues again. All of the other colleges are going with the Azure environment that we've built for this. But I understand your concern. If you have any more questions, I'm happy to help or explain more.

Thanks,

Ankoni Lowman

From: Alfred, Marcus <marAlfred@Howard.edu>
Sent: Monday, February 7, 2022 11:36
To: Osaghae, Olga <olga.osaghae@howard.edu>; Ankoni Lowman <alowman@gocloudforce.com>
Subject: Meeting follow up

Good morning VP Osaghae and Dr. Lowman,

Sorry for the delay. Last week got away from me. I wanted to say thank you for the meeting a week ago Friday and also follow up.

1.Our main priority is to re-establish our network in the CPL. We had our own subdomain for over 30 years 138.238.192 for research and training students in HPC, networking, and programming. With the Navy grant, we were supposed continue and revamp this work. So please

either give us back this subdomain which we'll administer, or help us get our own external connection.

This helps with both the COAS cluster and the Navy award.

2.I wanted to make sure i didn't misunderstand in our meeting. So there are no university contractual issues that stops us from using an outside vendor like comcast or t mobile to get an external connection? And the current vendor "k-something" isn't working out to well?

3.I've attached our quote for the HPC system. We've changed it from a workstation to a rackmount.

4.I'd like the connectivity for azure so that we can connect using machines in our lab.

Please let us know if it's possible to re-establish the 192 subdomain (we did DNS, security, etc.) or what you all can do to help with an external ISP research connection. If none of these work, we'll have to do something else.

Thanks again,

Marcus Alfred
Pronouns: he, him, his
Associate Professor
Howard University
Dept. of Physics & Astronomy
Washington, DC 20059
202-806-6258
maralfred@howard.edu