Compliant Cloud+Campus Hybrid HPC Infrastructure

Brenden Judson
Computer Science and Engineering
University of Notre Dame
bjudson1@nd.edu

Matt Vander Werf, Paul Brenner
Center for Research Computing
University of Notre Dame
{mvanderw,paul.r.brenner}@nd.edu

***Abstract*—We present a hybrid cloud+campus model for deploying secure research cyberinfrastructure in line with a growing number of federally funded scientific research security requirements. While the security mechanisms are inline with many regulations, we specifically focus on the NIST 800-171 CUI compliance that is now required by many US DARPA funded contracts. We discuss our architectural framework and rationale for leveraging shared ND services in AWS GovCloud in concert with CUI compliant HPC systems on our campus in a hybrid fashion; allowing an individual CUI regulated research project to bridge two connected but distinct infrastructures.**

***Index Terms*—CUI, FISMA, HPC, NIST, AWS GovCloud, NIST SP 800-171, Thin Client**

I. Introduction

The widespread embrace of distributed and data-centric platforms such as the Internet of Things (IoT), cloud storage, machine learning, etc. has been driving high performance computational research infrastructure, which has traditionally been computation-centric, toward data-centric models. Worldwide, the amount and diversity of data continues to grow exponentially. A recent prediction, made by the International Data Corporation (IDC), claimed that by the year 2025, 163 zettabytes of data will be created globally each year [1]. As such, it is getting increasingly difficult to contain and regulate. Recent news stories surrounding data privacy laws such as Facebook's Zuckerburg hearing before congress [2], “fake news” influence of democratic elections, and others like them have brought the value, risk and power of leveraging data to the forefront of society's attention (including legislators); making data regulation increasingly more important and commonplace.

While society's attention to data security has recently increased, the federal regulation of sensitive digital data is not a new government focus. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) placed regulations on medical information. Similarly, personally identifiable information (PII) and classified information have been highly regulated for decades. Major strides towards regulation were taken in 2002 when the Federal Information Security Management Act (FISMA) became law, requiring federal agencies to develop, document, and implement an information security and protection program (revised on December 8, 2014) [3]. FISMA tasked the National Institute of Standards and Technology (NIST) to create standards outlining how to properly implement an information security and protection program. On November 4, 2010, President Barack Obama issued Executive Order 13556 with the goal of establishing an “open and uniform program for managing” controlled unclassified information (CUI) [4]. Federal agencies often contract with private organizations, resulting in some their sensitive data being housed externally. This led to the creation of NIST Special Publication (SP) 800-171 Rev. 1 in 2016, which set the regulation standards for CUI [5] data resident in non federal IT infrastructure. Since then, a growing number of agencies have been requiring companies and institutions housing their information to meet NIST SP 800-171 requirements, often referred to as CUI compliance. Specific to the research projects in this work, the Defense Advanced Research Projects Agency (DARPA) requires CUI compliance for many of their projects. Multiple federal grants at the University of Notre Dame (ND) now have the requirement of CUI compliance.

As CUI compliance continues to become the norm when working with certain federal agencies; many companies, universities, and institutions look to make their information systems CUI compliant. Recent work highlights this trend and how compliance has become such a relevant topic. For example, in the HPC Security & Compliance Workshop (PEARC18), Pennsylvania State University's Joseph Gridley gave a presentation on the “Validation of CUI Environments Using NIST 800-171A” [6] and Preston Smith outlined the University of Purdue's compliant environment in his presentation, “REED: from Service to Ecosystem” [7]. This workshop featured many other relevant presentations that can be found on their website [8]. Other work such as Kelly W. Bennett's paper on a cloud-based security architecture [9] and the University of Arizona's CUI compliant environment [10] are additional examples of other institution's work that pertains to compliance. Although there is a great deal of relevant work being done, there is very little documentation or published work on hybrid compliant environments.

As outlined by NIST SP 800-171, there are fourteen categories associated with being CUI complaint:

1) Awareness and Training
2) Auditing and Accountability
3) Configuration Management
4) Identification and Authentication
5) Incident Response

6) Maintenance
7) Media Protection
8) Personnel Security
9) Physical Protection
10) Risk Assessment
11) Security Assessment
12) System and Communication Protection
13) System and Information Integrity
14) Access Control

Each one of these categories is broken down into many controls that specify the exact compliance requirements, for more details see [11].

In recognition of the expanding market for cloud services that meet various federal regulations, all three of the major US public cloud vendors have taken strides to expand this aspect of their business [12] [13] [14]. The University of Notre Dame's CUI environment utilizes the Amazon Web Services (AWS) GovCloud region to implement a compliant environment and therefore, AWS is the cloud vendor focused on for the remainder of this paper. AWS GovCloud (US) is an isolated AWS region designed to allow customers to move sensitive workloads into a cloud environment that addresses their specific regulatory and compliance requirements. The region is operated exclusively by employees who are U.S. citizens, only on U.S. soil, and is only accessible to vetted U.S. entities. While not all CUI regulated projects have a US citizenship requirement, it is a common requirement to meet certain federal regulations, including International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR). These GovCloud features (along with others) allow AWS to help customers meet a variety of compliance requirements such as HIPAA, ITAR, EAR, Federal Risk and Authorization Management Program (FedRAMP), FISMA High Baselines and the DOD Security Requirements Guide.

Recent research grants that the University of Notre Dame has become involved with, such as those sought by the ND Turbomachinery Laboratory (NDTL) [15], have provided the unique opportunity to create a hybrid (cloud+campus) CUI environment that contains the necessary infrastructure to perform high performance computing (HPC). This paper continues by comparing the trade-offs between hosting a CUI HPC environment in AWS GovCloud or with on-campus hardware. From there, we outline Notre Dame's hybrid CUI solution which attempts to take advantage of the benefits of AWS GovCloud while performing top-tier HPC in an on-campus environment.

II. Cloud+Campus Trade-offs

A. Cloud CUI Environment

As was previously mentioned, AWS GovCloud helps customers meet a variety of security regulations. Outsourcing your compliant environment's infrastructure to AWS GovCloud typically means you have less to manage because multiple regulation requirements are covered by AWS. This can simplify your responsibility in meeting compliance, saving you time and money. Cloud services also help you avoid the headaches that accompany having physical hardware on-site (compliance audits, maintenance, deterioration, etc.). Instead, the cloud vendor assures you state-of-the-art hardware and enhanced security measures. Large public clouds may also have newer and more powerful individual servers than in the average HPC environment (an optimized InfiniBand network is a separate matter). One of the reasons for this is the fact that many companies and organizations have been keeping their on-site HPC systems longer than ever before [16].

Cloud technologies are also more elastic and scalable than traditional on-campus HPC infrastructures. Being able to scale with demand provides agility to your CUI environment that has not been available in the past, providing users with more options. For many customers, AWS allows them to scale beyond what would be practical in their on-campus environments without the need for large capital investment. AWS also offers cost saving features such as spot instances, which allow you to purchase spare compute capacity at steep discounts.

B. Campus CUI Environment

Today, most aspects of enterprise information technology (IT) at ND have been widely migrated to the cloud. HPC is also gaining traction in cloud usage. Cloud spending by HPC customers grew by 44 percent from 2016 to 2017 and it is projected to be the fastest-growing expense for HPC centers for the next five years, reaching nearly $3 billion by 2022 [16]. All three major cloud providers now support some degree of HPC [17] [18] [19] and the case for HPC in the cloud is growing ever stronger. However, all three lack the capability to cost effectively support the large scale (>1-10K tightly coupled cores) and high utilization rates typical of top-tier HPC centers operated by many research institutions such as Notre Dame.

HPC environments consistently have very high utilization percentages, much higher than general or enterprise IT systems. Cloud services are priced based on their utilization and thus, cloud cycles continue to be more expensive than in-house cycles for HPC [16]. Furthermore, hosting your secure infrastructure in the GovCloud region adds additional fees to AWS's standard fees. Many customers will find that their research computing infrastructure is cheaper to host locally as we found for one particular research case in our prior work [20]. We can do a quick price evaluation to prove this point. To implement an infrastructure capable of top-tier HPC, administrators at the University of Notre Dame recently purchased 21 servers (each with 48 cores, 128 GB RAM and Infiniband network) priced at $6,950 per server for a total cost of $145,950. Note that additionally our facility and utility costs for this size system adds $20K annually in operating costs. This can be compared to reserving AWS GovCloud instances at their current price (pricing is accurate as of Sept. 2018) [21]. If you pay upfront, the c5.9xlarge instance type (36 core, 72 GB RAM) running a RHEL OS (same OS as Notre Dame's servers) is available to reserve for 3 years at $20,148 per instance, allowing you to make a 3 year reservation of 21 less powerful servers for a total cost of $423,108 (21 * $20,148 = $423,108). Not only is the figure more than double the cost of purchasing physical hardware, but the reservation only lasts for 3 years while the typical turnaround on servers at Notre Dame is approximately 5-6 years. Due to the high utilization requirements of HPC and the current pricing model for cloud resources, a greater amount of capital is required to leverage a cloud HPC environment.

Additionally, HPC applications notoriously require very fast storage and extremely low latency network performance. Alongside the absence of readily configured high performance file systems such as Lustre or Panasas, network performance is one of the main reasons for top-tier HPC's lack of adoption of the cloud model. The use of MPI and RDMA on InfiniBand interconnects permits efficient execution of the diverse set of highly parallel jobs typical of top-tier HPC environments. These inter-network speeds are not currently matched by an AWS service. Azure attempts to fill the niche by offering InfiniBand interconnects [22] but fails to capture the market space due to high costs [23].

III. ND Hybrid Solution

After much consideration, ND decided to implement a hybrid CUI compliant environment. We refer to this implementation as a hybrid environment because its infrastructure is hosted both in AWS and in an on-campus data center. AWS GovCloud is where the majority of this environment's logical components are hosted. This allows Notre Dame to take advantage of the simplicity and scalabilty offered by AWS. Due to the cost of hosting HPC in AWS and concerns surrounding the inter-network speed, HPC computations are supported via on-campus hardware residing in our research computing data center.

The following section outlines the various aspects of Notre Dame's implementation by walking through a typical production use case of a client establishing a connection to a workstation housed in the cloud environment and from there, leveraging HPC in the on-campus environment. This use case is illustrated in Fig. 1.

A. Client-Facing

The client-facing portion of the implementation (found in the top right corner of Fig. 1) leverages Ericom Connect for access management. A client has three interface options when attempting to establish a connection: AccessPortal (HTML-5 based RDP application), AccessToGo (mobile RDP application) and AccessPad (desktop RDP application). Using one of these products, a client may authenticate as a user in ND's separate CUI specific Active Directory domain *risc.nd.edu*. Before establishing a connection with the Ericom Gateway (a bastion host housed in Shared Services), a client must also use Duo Authentication for 2-factor authentication (2FA).

Once connected, Ericom's interface offers the user an isolated RDP environment, allowing them to remotely access a workstation. It is important to point out that the client-facing portion of the environment has a very restricted connection. This connection is so minimal that the client's local machine can be referred to as a “zero client”, i.e. the only data sent to the local machine is pixel values. File transfer between the two machines is not an offered service.

B. Shared Services

Shared Services (as shown in top left corner of Fig. 1) is an AWS GovCloud VPC contained in an isolated account. The Shared Services VPC offers services to other accounts via a VPN peering connection. These services currently include hosting the domain, Duo Authentication, Windows Server Update Service (WSUS), Nessus Vulnerability Scanner, System Center Configuration Manager (SCCM), Red Hat Satellite Server, and the Ericom Connect Server.

As mentioned, the client facing portion of the implementation ultimately ends up at the Ericom Gateway. This is housed in the Shared Services public subnet. From the gateway, the connection is then directed to the Ericom Connect server in the private subnet of the Shared Services VPC. Through a VPN peering connection, the server is then able to connect to the appropriate project's VPC.

C. Project VPCs

Each project is separated into its own AWS account (example VPCs can be found in the bottom left corner of Fig. 1), thus, isolating the billing, logging and responsibility to the corresponding project. Within the account, each project has a VPC containing all of its cloud resources (albeit it may utilize Shared Services' resources). The VPCs are generated with Cloud Formation scripts, promoting re-usability, scalability, agility, transparency, and security. It is within these VPCs that the EC2 instances containing the users' workstation(s) are housed. Users may start and stop their workstations, however, administrative access is required to launch or terminate instances (i.e. all users can pause instances but may not create or delete them).

There is a major focus to secure the transmission of data in and out of these zones. Notre Dame's Office of Information Technologies (OIT) took many steps to ensure the reliability and security of data transmission. In the public subnet of each VPC, there is a VPC NAT Gateway. This service acts as the bridge between the VPC's public and private subnet and it is through the NAT Gateway that the client's RDP connection (through Ericom) is directed to workstations housed in the private subnet. The gateway ensures that access to the various services in the private subnet is only given to trusted, authenticated connections and that their access is isolated to the specified service.

The transfer of actual data (i.e. beyond an RDP connection) into and out of the CUI GovCloud environment is closely monitored and controlled. Any data transfer into the CUI GovCloud environment from the outside world must abide by four requirements for compliance: (1) the data transfer must be

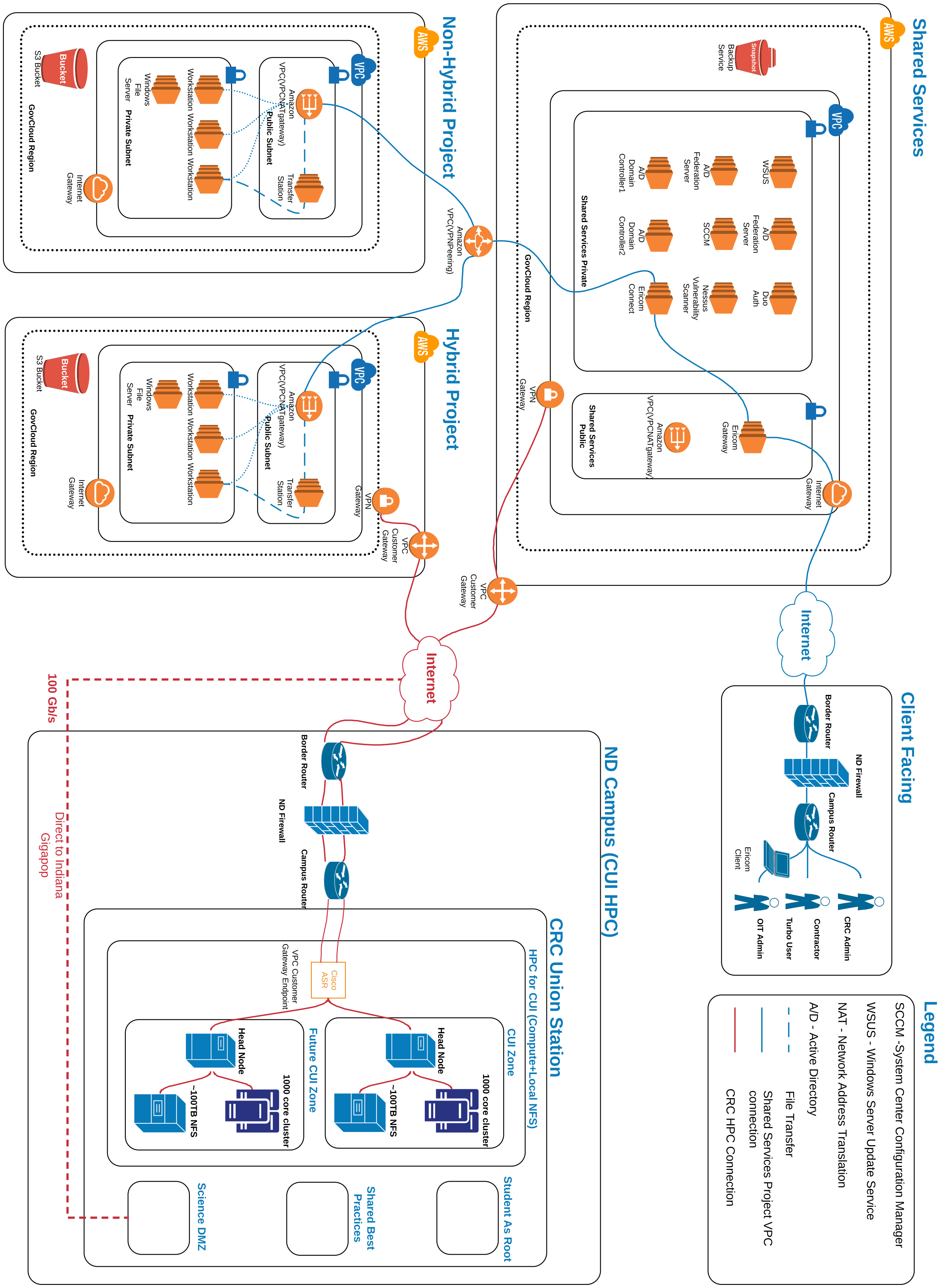

Fig. 1. Graphical representation of the University of Notre Dame's Hybrid CUI environment.

initiated from a secure and trusted system, (2) the data transfer must be compliant with Federal Information Processing Standards (FIPS) Publication 140-2 encryption requirements, (3) the file transfer must be logged, and (4) the authentication used to perform the file transfer must be logged. Given these requirements, one can envision multiple physical solutions that could be used. For the NDTL project VPC, the chosen solution requires that only ND-managed systems are used to transfer data into the CUI GovCloud environment. For this solution, authenticated users transfer data using only secure, FIPS 140-2 compliant file transfer tools to secured AWS S3 buckets located within the NDTL project VPC. Once the data is in the S3 buckets, it is then synced to file servers within the NDTL project VPC. These file servers then serve the data to appropriate NDTL workstation instances. The S3 buckets are white-listed to only allow connections from specific trusted IPs and authorized users. Utilizing S3 buckets in this way allows for all the required logging to be performed appropriately. A direct transfer path to the workstation instances from the S3 buckets could also be envisioned if there were sufficient software tools to ensure the four compliance measures above.

The transfer of CUI data out of the GovCloud CUI environment is much more restricted and limited. Within each project VPC's public subnet, there is a special transfer station instance that is only used for transferring data out of the GovCloud CUI environment. All outbound data transfer must go through the transfer station instance, which is white-listed to only allow outbound connections to a very select group of trusted, authorized IP addresses of data store portals designated by the sponsoring agencies of the project. Only select authorized users are permitted to use the transfer station instance.

AWS Cloud Watch keeps extensive logs on a per account basis, providing each project VPC with its own set of logs. Using tools such as AWS Cloud Trail and an SNS topic, we plan to have automated alerts and updates that are sent to OIT staff. This is discussed in the Future Work section of this paper.

D. Secure Cloud+Campus Bridge

Because HPC computations are executed on the campus resident HPC hardware, the corresponding project VPCs need a secure connection to the on-campus infrastructure. Notre Dame's Center for Research Computing (CRC) and OIT worked together to ensure the security of this bridge. The keystone of this effort was purchasing a Cisco ASR network appliance [24]. The ASR creates two separate encrypted tunnels. One tunnel is between the HPC CUI environment and Shared Services (giving HPC CUI environment access to Shared Services resources like DNS, NTP, Red Hat OS updates, etc.); the other connects the HPC CUI environment to the corresponding project VPCs. Each hybrid project VPC has a customer gateway pointing at the Cisco ASR appliance. The ASR is white-listed to only accept IPs known to be from the trusted project VPCs or the Shared Services VPC.

E. Campus HPC Infrastructure

Union Station Technology Center (USTC) is a multi-tenant data center, privately operated by Global Access Point. It is within USTC that the CRC's HPC resources and CUI compliant zone are housed (as shown in bottom right corner of Fig. 1).

All CRC machines housed in USTC are logically separated into one of four security regions: student as root, science DMZ, general best practices, or CUI compliant. “Student as root” is a sandbox environment which gives administrator access to users who are not CRC system administrators. Research projects housed in the CRC that incorporate techniques requiring transmission of very large data sets with external peers (such as high energy physics) are placed in the science DMZ zone. This zone has large bandwidth and a direct connection to Indiana GigaPop to facilitate the large uploading/downloading of these data sets. “Best practices” is an environment where the CRC's security best practices are applied and the research project data sets do not have a specified elevated security requirement. It is the largest of the four zones and the most actively used, seeing approximately four fifths of the CRC's computing workload.

The final zone is the newly established CUI compliant zone, where the CUI compliant HPC resources are housed. Each project, in the CUI compliant zone, is separated into an isolated subnet and has a head node for establishing a connection with the Cisco ASR. Along with the head node, each project subnet has an HPC cluster and a NFS server. The HPC cluster is interconnected with an InfiniBand switch [25] providing the inter-network speed that is required for many HPC environments.

IV. State of Implementation and Component Validation

Notre Dame's OIT and CRC have worked together to deploy a hybrid CUI compliant environment enabling cost-effective HPC. This environment is currently the home for DARPA funded grants with CUI and HPC components.

A. Shared Services & NDTL Project VPCs

The Shared Services VPC was designed implemented over the course of two years and has been in production use since January 2018. It was implemented and is managed by Notre Dame OIT, specifically the Information Security & Compliance and the Identity & Access Management Services groups within OIT. All inbound and outbound network traffic between the GovCloud, campus CUI environments and outside world must go through the Shared Services VPC, where such traffic is heavily monitored and controlled.

The Shared Services VPC contains various administrative services and tools that are utilized by the project VPCs in the GovCloud environment and by the on-campus CUI HPC environment. Most importantly, it provides the ability for users and administrators to access the GovCloud and on-campus CUI environments in a secure and CUI compliant manner.

Alongside the Shared Services VPC, the VPC for the NDTL project (“Hybrid Project GovCloud” in Fig. 1) has also been in production use since January 2018. It was created by OIT and is managed by OIT and Notre Dame's Engineering & Science Computing (ESC) group. It is within this VPC that workstations for the NDTL group are housed. These workstations are used for small computational models and graphics-intensive data analysis and are also used to access the on-campus CUI HPC environment.

B. Campus CUI HPC Environment

Over the past year, CRC engineers have implemented the on campus CUI compliant HPC environment at the USTC data center. Prior to implementation, the CRC performed multiple extensive reviews of the 110 CUI controls and developed plans for fulfilling all the CUI requirements. These plans for fulfilling the requirements were also been reviewed by the CRC's internal security group.

The secure on-campus CUI environment is enclosed in racks that are locked and only accessible via special RFID proximity access cards. The racks are fitted with an APC NetBotz rack monitoring appliance [26] that controls who can access the racks and keeps track of all access logs for auditing purposes. The appliance also can send out alerts if there are any unauthorized accesses or forced entries to the racks (including failed attempts).

As mentioned previously, the HPC environment includes HPC compute nodes, an interactive frontend node, an NFS server, and several other administrative systems. The administrative systems include systems for managing/provisioning the other systems in the environment (using the open-source xCAT provisioning and management software) and to help fulfill CUI requirements. The HPC compute nodes (and frontend node) have both 10 Gb Ethernet and 100 Gb EDR InfiniBand network connections, connected to a Cisco network switch and a Mellanox EDR InfiniBand switch, respectively. All the systems are running Red Hat Enterprise Linux (RHEL) 7 for the operating system and Univa Grid Engine (UGE) software is being used as the job scheduler for the HPC environment. The NFS server is used for scratch storage and is mounted on the frontend node and the compute nodes. Persistent data resides only in the AWS GovCloud environment.

The open-source Xymon monitoring software is used to monitor health of the systems in the on-campus HPC environment, including CPU load, memory usage, disk usage, and network connectivity. While the Xymon server component resides in the Shared Services VPC, each system in the on-campus HPC environment has a Xymon client package installed, reporting system health data to the Xymon server.

To help with CUI compliance, several software tool-sets are utilized in the on-campus HPC environment as well. These include a Graylog server for log aggregation, management, and monitoring and Tripwire Enterprise for change monitoring, among others.

C. Campus Bridge

The on-campus CUI HPC environment and the AWS GovCloud CUI environment are connected via multiple encrypted tunnels via the use of a Cisco ASR network appliance. This Cisco ASR appliance resides in the on-campus CUI environment. At present time, there are two encrypted tunnels in use, one between the on-campus HPC environment and the NDTL project VPC and the other between the on-campus HPC environment and the Shared Services VPC. Any additional similar hybrid projects will also each have two encrypted tunnels using the same Cisco ASR appliance, one connecting to Shared Services and the other connecting to the corresponding project VPC. The only way to access the on-campus CUI HPC environment over the network is via these encrypted tunnels.

All data transfer with the outside world must go through the AWS GovCloud CUI environment (as discussed previously). Once the data is in the GovCloud CUI environment, users can then transfer the data they need to perform top-tier HPC using secure transfer tools (such as SFTP) to the storage systems in the on-campus CUI HPC environment. Data can also be transferred back to the GovCloud CUI environment in a similar fashion, as necessary. This data transfer traverses the appropriate encrypted tunnel(s) connecting the GovCloud CUI environment and the on-campus CUI HPC environment.

V. Future Work

The University of Notre Dame has created a new, complex environment that will demand a great amount of attention and effort to maintain. Furthermore, there are many areas for improvement that have been identified and we plan on exploring. For these reasons, the following section has been included to highlight the future work pertaining to this project.

A. Audits and Shared Responsibility

Ensuring that an environment will pass a random audit can be a detail-oriented and meticulous task; it should prove to be one of the major sources of future work. For example, any new user/administrator must go through security training, only vetted individuals may have access to the compliant hardware, etc. That being said, the University of Notre Dame's amount of future work in this area has been greatly reduced by implementing a hybrid solution. By using cloud services to implement our CUI compliant environment, we adopt a “shared responsibility model”, implying that the responsibility of qualifying as CUI compliant is now shared between the cloud vendor and the customer. Fig. 2 provides an overview of the “shared responsibility model” for Notre Dame's environment.

In order to further enhance and simplify the audit process, we plan to leverage AWS Config in our implementation. “AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources.” [27] With this service, we would have detailed resource configuration histories and be alerted of any configuration changes, thereby, helping to ensure CUI compliance.

B. Additional Projects

The recent push for data regulation, alongside NDTL's and Notre Dame's continued pursuit of sensitive grant proposals,

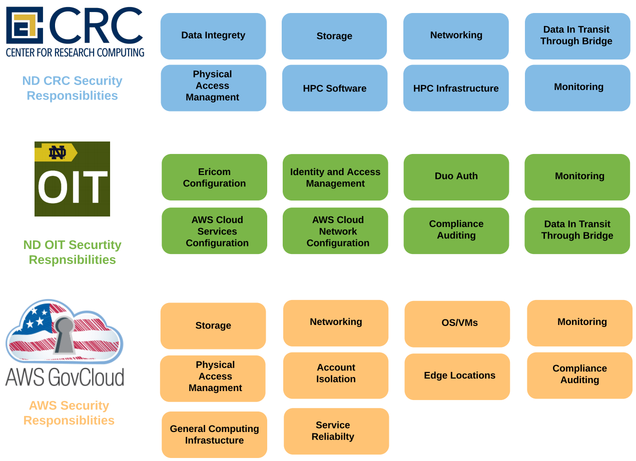
CRC
CENTER FOR RESEARCH COMPUTING
ND CRC Security Responsiblities
Data Integrety
Storage
Networking
Data In Transit Through Bridge
Physical Access Managment
HPC Software
HPC Infrastructure
Monitoring
OIT
ND OIT Securtity Respnsibilities
Ericom Configuration
Identity and Access Management
Duo Auth
Monitoring
AWS Cloud Services Configuration
AWS Cloud Network Configuration
Compliance Auditing
Data In Transit Through Bridge
AWS GovCloud
AWS Security Responsiblities
Storage
Networking
OS/VMs
Monitoring
Physical Access Managment
Account Isolation
Edge Locations
Compliance Auditing
General Computing Infrastucture
Service Reliabilty

Fig. 2. Outline of the Responsibility Distribution

leads us to believe there will be more future projects requiring CUI compliance. Scaling the University's CUI compliant environment with demand should prove to be another significant source of future work.

The simplicity, agility, and virtually unlimited nature of cloud services makes the cloud portion of our environment easy-to-scale. Cloud Formation is utilized to deploy the the cloud environment on a per project basis (i.e. each project has it's own Cloud Formation stack). Utilizing Cloud Formation provides automation helping to make our environments more secure, reusable, reliable, and easy-to-scale. Scaling is much more involved with the on-campus portion of our environment (e.g. creating network tunnels, setting up general data center infrastructure, etc.).

C. Maintenance

As with any infrastructure, system maintenance and failures are to be expected and thus, the maintenance of our environment is a final, major source of future work. It is important to point out that cloud vendors handle the maintenance of their devices meaning the hybrid model greatly reduces the amount of maintenance required. It is the on-campus portion of our solution that will require the most maintenance. As mentioned before, we will be using a Red Hat Satellite server located in Shared Services to help manage RHEL OS updates for our on-campus CUI environment. Other than that, system health inspections, repairing hardware failure etc. should be expected on a regular basis and will require moderately more logging and controls than we use in our other three security zones in the CRC.

VI. Conclusion

Big data paradigms like social sensing, machine learning, etc. have helped to highlight the power behind leveraging data in computational research. Now more than ever digital data is seen as a highly valued asset that needs to be protected and regulated. As such, government regulation on data security practices is becoming increasingly commonplace; this is especially true for federally associated data. Because of the growing amount of regulation, organizations seeking federally funded business opportunities, grants, etc. should ensure compliant practices. Even if the federal associated data is not currently regulated, recent trends suggest that depending on its sensitivity, it may be in the near future. There are a wide-ranging number of federal regulations on data security for research institutions; this paper focused on CUI compliance which has its primary requirements outlined in NIST SP 800-171.

We gave an initial description of our CUI compliant hybrid cyberinfrastructure at ND. It is hybrid in the sense that the environment's general IT infrastructure is housed in the cloud but it places HPC workloads in a campus CUI environment through a secure, encrypted tunnel. This paper can serve as a starting place for someone looking to implement their own compliant environment. CUI compliance follows today's best practices so it can also be a guideline for less stringent regulations or for someone who is just looking to improve their data security practices.

The hybrid model fits well in today's landscape. By housing the environment's backbone in the cloud, we promote agility, scalability, and simplicity, not to mention the other benefit one gets from leveraging cloud services (state-of-the-art hardware, enhanced security measures, smaller capital requirements, etc.). However, the top-tier sustained HPC that is done by today's research community is still economically impractical to perform in the cloud. A hybrid solution allows you to cost effectively perform HPC while still getting the benefits that come with migrating your general/enterprise IT to the cloud.

Acknowledgment

Building a secure research cyberinfrastructure with a complex set of capabilities requires the coordinated teamwork of numerous subject area experts. The model discussed in this paper could not have been realized without the contributions of: Rich Sudlow, Steve Bogol, Scott Hampton, Jacob Bonek [Notre Dame CRC], Kolin Hodgson, Bob Richman, Bob Winding, Mike Rowland, Sharif Nijim [Notre Dame OIT], and Lisa Berlincourt [Notre Dame ESC].

References

[1] D. Reinsel, J. Gantz, and J. Rydning, “Age 2025: The evolution of data to life-critical dont focus on big data; focus on the data thats big,” An IDC White Paper, Sponsored by Seagate, 5 Speen Street, Framingham, MA 01701, Tech. Rep., April 2017.

[2] (2017, April) Facebook, social media privacy, and the use and abuse of data. U.S. Senate. [Online]. Available: https://www.judiciary.senate.gov/meetings/facebook-social-media-privacy-and-the-use-and-abuse-of-data

[3] (2014) Federal information security modernization act. National Institute of Standards and Technology. [Online]. Available: https://csrc.nist.gov/topics/laws-and-regulations/laws/fisma

[4] (2010) 3 cfr 13556 - executive order 13556 of november 4, 2010. controlled unclassified information. U.S. Government Publishing Office. [Online]. Available: https://www.gpo.gov/fdsys/granule/CFR-2011-title3-vol1/CFR-2011-title3-vol1-eo13556

[5] (2016) Protecting controlled unclassified information in nonfederal systems and organizations. National Institute of Standards and Technology. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final

[6] J. Gridley, "Validation of cui environments using nist 800-171a," presented at the HPC Security & Compliance Workshop (PEARC18), July 2018.

[7] P. Smith, "Reed: from service to ecosystem," presented at the HPC Security & Compliance Workshop (PEARC18), July 2018.

[8] (2018, July) Hpc security & compliance workshop (pearc18). University of Florida Research Computing. [Online]. Available: https://www.rc.ufl.edu/research/events/workshop-pearc18/

[9] K. W. Bennett, D. W. Ward, and J. Robertson, "Cloud-based security architecture supporting army research laboratory's collaborative research environments," in *Proc. SPIE Defense & Security Volume 10635*, Orlando, Florida, May 2018.

[10] (2018) Controlled unclassified information (cui) environment. University of Arizona. [Online]. Available: https://it.arizona.edu/cui

[11] (2017) Official cui policy documents. Federation of American Scientists. [Online]. Available: https://fas.org/sgp/cui/index.html

[12] (2018) What is aws govcloud. Amazon Web Services. [Online]. Available: https://docs.aws.amazon.com/govcloud-us/latest/UserGuide/whatis.html

[13] (2018) Azure government. Microsoft Azure. [Online]. Available: https://azure.microsoft.com/en-us/global-infrastructure/government/

[14] F. Konkel. (2018, March) Google cloud targets federal government. [Online]. Available: https://www.nextgov.com/it-modernization/2018/03/google-cloud-targets-federal-government/146917/

[15] (2018) Turbomachinery laboratory. Notre Dame Turbomachinery Laboratory. [Online]. Available: https://turbo.nd.edu/

[16] M. Feldman. (2018, June) Cloud computing in hpc surges. [Online]. Available: https://www.top500.org/news/cloud-computing-in-hpc-surges/

[17] (2017) High performance computing. Amazon Web Services. [Online]. Available: https://aws.amazon.com/hpc/

[18] (2018) High performance computing. Microsoft Azure. [Online]. Available: https://azure.microsoft.com/en-us/solutions/high-performance-computing/

[19] (2018) High performance computing. Google Cloud. [Online]. Available: https://cloud.google.com/solutions/hpc/

[20] B. Judson, G. McGrath, E. Peuchen, M. Champion, and P. Brenner, "Cloud iaas for mass spectrometry and proteomics," in *Proc. ACM Symposium on High Performance and Distributed Computing HPDC, ScienceCloud17*, Washington D.C., USA, June 2017.

[21] (2018, September) Amazon ec2 reserved instances pricing. Amazon Web Services. [Online]. Available: https://aws.amazon.com/ec2/pricing/reserved-instances/pricing/

[22] E. Karpilovski. (2014, February) Infiniband enables the most powerful cloud: Windows azure. [Online]. Available: http://www.mellanox.com/blog/2014/02/infiniband-enables-the-most-powerful-cloud-windows-azure/

[23] C. Downing. (2018, March) How the cloud is falling short for hpc. [Online]. Available: https://www.hpcwire.com/2018/03/15/how-the-cloud-is-falling-short-for-research-computing/

[24] (2017) Cisco asr 1001-x router. Cisco Systems. [Online]. Available: https://www.cisco.com/c/en/us/products/routers/asr-1001-x-router/index.html

[25] (2018) Mellanox infiniband edr switch series - overview. Mellanox. [Online]. Available: https://http://www.mellanox.com

[26] (2018) Netbotz rack monitor 570. APC by Schneider Electric. [Online]. Available: http://www.apc.com/shop/us/en/products/NetBotz-Rack-Monitor-570/P-NBRK0570

[27] (2018) Aws config. Amazon Web Services. [Online]. Available: https://aws.amazon.com/config/

APPENDIX

A. *Abstract*

"Figure 1 in the paper covers the system architecture. This paper is not paired with an additional artifact."