Office of the Vice President
and Chief Financial Officer
Procurement Services
https://procurement.ufl.edu/

971 Elmore Drive
PO Box 115250
Gainesville, FL 32611-5250
(352) 392-1331 Fax 352-392-8837

January 14, 2022

ADDENDUM #1 to the University of Florida ITN22NH-124 HITRUST Certification for HiPerGator Supercomputer scheduled to be opened on **January 27, 2022 3:00 PM** at the University of Florida, Elmore Hall Conference Room, Radio Road, Gainesville, Florida.

This addendum shall be considered part of the Contract Documents for the above mentioned **ITN22NH-124** as though it had been issued at the same time and incorporated integrally therewith. Where provisions of the following supplementary data differ from those of the original document, this addendum shall govern and take precedence. All other terms, conditions, and regulations will apply.

This addendum consists of:

1. **Responses to technical questions and inquires submitted prior to 5:30pm, January 6, 2022.**

Sincerely,

Nicola Heredia

Nicola Heredia, Director
Procurement Services

Please acknowledge receipt of Addendum #1 by signing below and returning this addendum with your proposal. Failure to include addendum with your proposal may result in rejection.

_____   _____
Signature   Company Name

_____
Email Address

_____   _____
Company Address   City/State/Zip

The Foundation for The Gator Nation

An Equal Opportunity Institution

Q1.   What industry standards have you used in which to base your program and policy (outside of your regulatory requirements, e.g. ISO, NIST)? Is the HiPerGator supercomputer in compliance with any other frameworks? (e.g., SOC, NIST 800 series)

A1.   HiPerGator is compliant with most controls of NIST 800-53 moderate except for the following controls that require action: AC-12, AU-3, SC-12, SC-13 and intrusion prevention system (IPS) and advanced persistent threat (APT) monitoring need improvement.

Q2.   Please list the regulatory factors to be included in the scope of the HITRUST Validation.

A2.   HiPerGator needs to be certified to allow storage and processing of PHI data for research in compliance with HIPAA and HITECH,

Q3.   How many physical locations are currently operational?

A3.   one

Q4.   How many locations are involved in the storage, processing, and transmittal of your sensitive information that is in scope (which locations should be included within the assessment)?

A4.   one

Q5.   How many datacenters comprise HiPerGator?

A5.   one

Q6.   Is the HiPerGator Supercomputer completed segregated from other University systems?

A6.   HiPerGator connects to the Campus Research Network virtual environment, which is one of the virtual environments of the campus network. All access to HiPerGator goes over that network. HiPerGator itself includes numerous internal networks confined within the data center.

Q7.   Is the system accessible from the internet?

A7.   Yes

Q8.   Is any part of the scoped system hosted in the cloud?

A8.   No

Q9.   Is any part of the scoped system accessible by a third party?

A9.   There is a process for remote collaborators, who are not employees of UF to get access to allocation on HiPerGator under the sponsorship of UF personnel.

Q10.   How many interfaces are there to other systems?

A10.   There are no dedicated interface or connections to other systems, but as part of research projects temporary connections can be requested and are approved.

Q11.   Is the system publicly positioned?

A11.   Yes

Q12.   Can users access the HiPerGator Supercomputer from an external network not controlled by the University?

A12.   Access from the internet by authorized users is supported

Q13.   Do you use hardware tokens as an authentication method?

A13.   MFA uses DUO with the recommended device being a cellphone; hardware tokens are supported as an exception.

Q14.   Do you allow BYOD devices to connect to the HiPerGator Supercomputer?

A14.   Yes

Q15.   Do you have wireless access points in place at the in-scope facility?

A15.   No

Q16.   Does the scoped environment allow dial-up/dial-in capabilities (i.e., functional analog modems)?

A16.   No

Q17.   Is scoped information sent and/or received via fax machine (i.e., an actual machine, excluding efax or scan to email)?

A17.   No

Q18.   How many physical locations are there that house the people that administer HiPerGator, that would need to be interviewed?

A18.   Two locations, one on East Campus where the data center is located and another on main campus where some support staff is located.

Q19.   Do you do any information systems development (in-house or outsourced) for any of the HiPerGator Supercomputer system components?

A19.   No

Q20.   Does the scope of the project include HiPerGator 2.0 as well, or just HiPerGator 3.0?

A20.   The scope includes HiPerGator 2.0, 3.0, and AI (NVIDIA SupePOD) these are managed as a single system called HiPerGator; it does not include the secure environment HiPerGator-RV.

Q21.   Is the goal to certify the entire environment around HiPerGator or just Gatortron?

A21.   The entire HiPerGator needs to be certified; GatorTron is just one research project.

Q22.   Understanding the starting point for the assessment to help increase maturity, assess HIPAA compliance, and provide an accurate timeline for HITRUST certification would be helpful. How would you rate the overall cybersecurity maturity and HIPAA compliance of the HiPerGator information security program?

A22.   About 8 out of 10.

Q23.   Do you have a document HIPAA Risk and Gap Analysis for HipPerGator currently?

A23.   We did an analysis of NIST 800-53 moderate and privacy controls, see Q1.

Q24.   Is this a first time certification?

A24.   Yes

Q25.   Has the University gone through a HITRUST assessment in the past and if so, can the report be shared with the bidders? If not, has the University undergone a scoping exercise to determine the number of potential requirements or a readiness assessment? Is this something the University would be interested in assistance with/inclusion within the proposal?

A25.   HiPerGator was subject to a HITRUST readiness assessment in summer of 2020. The report may be shared with the awarded vendor following execution of an NDA.

Q26.   Have you performed a readiness assessment or had a validated assessment performed using MyCSF? When was this done?

A26.   See Q25

Q27.   What version of the HITRUST MyCSF tool will be utilized for the Validated Assessment?

A27.   We prefer to use the latest version as this is a new activity. There is no need for backwards compatibility.

Q28.   Is the organization centralized (single entity) or does the organization have multiple (more than one) semi-autonomous business units? How many business units, if applicable?

A28.   HiPerGator is operated by UFIT as the single business unit.

Q29.   How is security coordinated across the organization?

A29.   The information security across the university is coordinated by UFIT.

Q30.   How many individuals are responsible for security, as applicable to the environment in scope?

A30.   About 10 people

Q31.   How many staff in IT? How many staff in security?

A31.   UFIT has about 350 permanent staff with about 20 in security and about 23 responsible for operating HiPerGator.

Q32.   Please provide an estimate of how many individuals would be involved in control requirement areas (e.g., walkthroughs).

A32.   3 people

Q33.   Does the University have a designated individual(s) that is or will be trained as a HITRUST CCSFP that will be a liaison for the selected vendor?

A33.   Yes

Q34.   Do you have any staff that will be assigned to the project that are familiar with the HITRUST methodology and the MyCSF platform? Do you anticipate having any university staff perform your readiness review in MyCSF or look to the vendor to complete?

A34.   The vendor should complete the readiness review and work with assigned staff. The readiness review of 2020 can be leveraged.

Q35.   Who has access to the patient records? Does it include students?

A35.   Patient records are associated with individual research projects, each with their own list of authorized and trained personnel, which may include students.

Q36.   Are there more than 5,000 users who could access this data?

A36.   Typical projects have fewer than 10 people. There can be 10 to 100 projects at any one time.

Q37.   Do any of the organization's personnel travel to locations the organization deems to be of significant risk?

A37.   Personnel does travel and such travel will be subject to risk analysis and approval on a project basis.

Q38.   Are your IT infrastructure/information assets centrally managed?

A38.   UFIT manages enterprise systems and HiPerGator; some distributed IT staff manage additional systems but these are out of scope.

Q39.   How many physical buildings/locations are in scope (This would include users and IT staff that assist in the security of the HiPerGator Supercomputer)?

A39.   User endpoints are not in scope

Q40.   How many applications that store, process, or transmit PHI are in scope? How many web applications that store, process of transmit PHI are in scope for this assessment? How many applications would be include in the HITRUST scope?

A40.   HiPerGator is research infrastructure supporting numerous applications including web applications. The applications are not in scope, the web servers are. When projects handling restricted data (PHI) their applications will be subject to separate risk and compliance assessment before approval.

Q41.   How many records of PHI are stored in the HiPerGator system? How many eventually will be? How many *unique* PHI records do you receive or transmit each year? (<10m, 10-60m, or >60m)?

A41.   Projects will be approved to handle records in the thousands; projects that involve millions of records will be required to use HiPerGator-RV.

Q42.   Is that PHI data also stored in your environment?

A42.   Only HiPerGator is in scope

Q43.   How many transactions/day or line items of data will be accessed?

A43.   This depends on the project, see Q41.

Q44.   What is the approximate number of appliances (firewalls, routers, switches, servers, workstations, IDS/IPS, Wireless Network Devices, WAPS) by operating system/platform in scope?

A44.   HiPerGator consists of about 1,000 appliances, most of them running a version of Linux, possibly a special-purpose Linux such as on network switches.

Q45.   What environment is in scope? (AWS, Azure, Oracle Cloud, on-prem, etc.):

A45.   Only HiPerGator is in scope, which is on-prem.

Q46.   Please list those vendors/third parties that are relied on to support the HiPerGator's operations (i.e., hosting providers, network service providers, etc.).

A46.   No external providers are in scope.

Q47.   Do you conduct application and network penetration testing?

A47.   Yes

Q48.   Do you conduct quarterly vulnerability scanning?

A48.   Yes

Q49.   Are security configuration reviews conducted on a regular basis (at least annually) for critical systems, infrastructure and devices?

A49.   Yes

Q50.   Is your internal network infrastructure segmented (e.g., firewalls or other access controls devices manage access to different part of the network)?

A50.   Yes

Q51.   Can a process flow diagram/overall network diagram/scoping document for the system in scope be provided?

A51.   Yes. The diagram may be shared with the awarded vendor following execution of an NDA.

Q52.   Is a current network diagram maintained that identifies all system components and access points in scope?

A52.   Yes

Q53.   Have you conducted an information security assessment or audit of your environment within the past six months? If yes, please describe.

A53.   Not for HiPerGator; HiPerGator-RV was assessed by an external assessor against NIST 800-53 moderate summer of 2021.

Q54.   Is it a requirement of the vendor to be a certified HITRUST assessor?

A54.   Yes

Q55.   Are you expecting the vendor to be on-site in Florida to perform the work? Due to these unprecedented times, many of our teams have been able to successfully work remotely with clients on Readiness and Validation engagements.

A55.   Being on-site is not a requirement.

Q56.   Do you envision a multiyear timeline to assess and remediate controls, before you gain HITRUST certification? Or do you believe you have the controls in place now to achieve HITRUST certification for HiPerGator right away?

A56.   We believe that we are close to achieve certification right away.

Q57.   Is there a required timeline that the University is looking to follow to get HITRUST certified? What is the University's target date for submitting an assessment to HITRUST for certification?

A57.   We hope to complete certification by Sep. 2022.

Q58.   Does Privacy need to be included?

A58.   This is a topic for negotiation.

Q59.   Is the University interested in performing a Readiness Assessment prior to beginning the HITRUST validation process?

A59.   A HITRUST Readiness Asssessment was performed in summer of 2020, see Q25.

Q60.   Is the University required to be certified on the b, i1 Assessment or r2 Assessment?

A60.   This is a topic for negotiation, we expect the need is for r2 assessment.

Q61.   Have you contracted with HITRUST to obtain a subscription to their MyCSF Portal?

A61.   Yes

Q62.   Have you conducted a self-assessment within the MyCSF Portal (owned by HITRUST)?

A62.   No

Q63.   What version of the HITRUST CSF are you planning to be certified (note: the most recent version is v9.6)?

A63.   V9.6 is preferred

Q64.   Does the University intend on testing the measured and managed control maturity ratings or just required passing maturity levels of policy, procedure and implemented? Does UF intend to assess measured and managed maturity levels?

A64.   This is a topic for negotiation. The university wants to consider testing measured and managed control maturity.

Q65.   Please provide the number of stakeholders and responsibility that are involved in this project internal and external to the University.

A65.   HiPerGator is infrastructure operated by UFIT with the CIO as responsible stakeholder to provide services to the university.

Q66.   How many people or groups of people would need to be interviewed to gain an understanding of the people, process and technology controls in place for HiPerGator?

A66.   Estimated at 10 to 20 people.

Q67.   Please provide a high-level overview of the technical architecture of the HiPerGator Supercomputer system.

A67.   HiPerGator is a Linux cluster architected for high-performance computing. It has compute nodes, login nodes, infrastructure nodes, webservers, storage systems, switches for Ethernet and InfiniBand.

Q68.   Is the HiPerGator system located in a university owned and managed Data Center, or a Data Center operated by a third-party?

A68.   HiPerGator resides in the UF data center.

Q69.   Do you have centralized security governance and is there a single set of policies and procedures for HiPerGator?

A69.   Yes and yes

Q70.   Do you feel you have an up-to-date, comprehensive set of IT and Security policies and procedures, or do you anticipate developing those being a key area of remediation?

A70.   We feel we have a reasonable set, possibly with some deficiencies

Q71.   Have policies and procedures for the HiPerGator environment been developed and documented specifically in consideration of the HITRUST requirements? If not, is the selected vendor expected to provide guidance to University employees on the development of such policies and procedures and/or recommend resources that can assist in their development?

A71.   This is a topic for negotiation.

Q72.   Does the HiPerGator maintain its own policies, procedures, and controls separate from the University?

A72.   All university policies and procedures apply and HiPerGator builds on these and adds to them.

Q73.   Do you use any part of the scoped system to sell goods or services?

A73.   No

Q74.   Are e-signatures utilized in the environment?

A74.   No

Q75.   Does the University have other systems that are HITRUST certified?

A75.   No

Q76.   Is any of the scoped information sent via courier, internal or external mail services?

A76.   No

Q77.   Does the University anticipate that the selected vendor will assist with assessing compliance with HIPAA beyond the scope HITRUST and/or facilitate compliance activities such as risk analysis, risk assessments, penetration testing, etc.?

A77.   No

Q78.   Will the Vendor be required to assess UF Information Technology documents?

A78.   Possibly if such documents are deemed relevant to HiPerGator certification.

Q79.   Does UF intend for the Vendor to propose on HITRUST readiness and implementation assistance services in addition to performing the Validation?

A79.   No

Q80.   Has the University developed a budget for this effort? If so, can you share that with the respondents?

A80.   The budget has not yet been fully finalized.

Q81.   Is this funded by a federal grant or under a prime federal grant?

A81.   No

Q82.   Is the UofF looking for or open to additional pricing to cover HIPAA and HITECH assessments in accordance with section 1.2 of the ITN document?

A82.   This is a topic for negotiation.

Q83.   Due to these unprecedented times, do you still require a hardcopy of the finalized proposal?

A83.   UF does require a hardcopy of the proposal.

Q84.   Depending on the response above, can we submit the proposal electronically via email or do you require a USB to also be submitted with the hardcopy?

A84.   Due to rules surrounding public procurement, UF does require the USB to be submitted with the hardcopy.

Q85.   Will the University accept electronic signatures on the original response due to COVID-19 protocols/office closures, or are manual signatures mandatory?

A85.   Electronic signatures are acceptable.

Q 86.   Does the selected vendor have the ability to negotiate the terms and conditions of the Contract for Services during Pre-Award Negotiations, or is that reserved only for the

University? Section 2.12 of the ITN indicates that the University may accept alternative terms or conditions, but we would like to confirm when that acceptance would have to occur.

A86.   The terms and conditions would be discussed and negotiated during the ITN process.

Q87.   Please clarify what type of text-weighted paper you request vendors to use for their submission. Also, do you have a preference on what post-consumer recycled content paper?

A87.   UF does acknowledge that it is asking for a hardcopy, but does ask that the vendor be as environmentally responsible as possible.

Q88.   Can proposing firms provide information in an Appendix section of the proposal (i.e., additional information)?

A88.   Yes

Q89.   In the "ADDITIONAL TERMS FOR INDEPENDENT CONTRACTORS" section of the Terms & Conditions, it states that all IP that results from the engagement belongs to the University, does that extend beyond the certification and deliverables we would provide to the University as a function of our HITRUST Certification process?

A89.   These are the standard terms used by UF. Terms may be negotiated to suit an individual contract such as this.

Q90.   We have a standard Indemnity that we provide to customers in regards to these services, would it be acceptable to start with that one should be selected and work with the University to reach a mutually acceptable indemnification provision?

A90.   Terms may be negotiated to suit an individual contract such as this.

Q91.   On page 7, 2.4 Pre-Award Negotiations: It states that the University has the right to negotiate prior to award for Terms and Conditions, however on page 11 4.1.1 Response Format, Tab 6 it is noted that UF may not negotiate terms not identified at time of submittal. Can you please clarify and confirm?

A91.   The vendor responses will be evaluated, with one of the evaluation criteria being the acceptance of UF terms and conditions. If there are modifications requested, it would be appreciated if they could be identified ahead of time, but they will be negotiated during the ITN process.

Q92.   Please comment on why the "Proposer is required to be in compliance with the requirements of the SAS 70 and/or Payment card Industry Data Security Standard".

A92. As per section 6.51 of the ITN document, this requirement is only relevant for e-commerce and/or credit card transactions. That is not relevant for this scope of work.

Q93. Will there be a pre-proposal conference call?

A93. At this point, there has not been a pre-proposal conference call scheduled.

Q94. Will there be a pre-proposal site visit?

A94. At this point, there has not been a pre-proposal site visit scheduled.

Q95. The RFP states that the University of Florida has an obligation to make the winning proposal public. Is it possible to have an exemption for any proprietary pricing and IP?

A95. The University is subject to the public records laws in the State of Florida. Any requests for release of information would be handled through the University of Florida Public Records Office.

Q96. Does the University of Florida have a sense or baseline, currently, on how well the HiPerGator program conforms to the HITRUST framework? If so, can you provide a grade on a scale of 1-10 with 10 being very high and 1 being very low?

A96. Estimated a grade of 8.

Q97. Are separate quotes for HITRUST preparedness and Validated Assessment desired?

A97. This is not a requirement.

Q98. If moving forward with the HITRUST Risk-Based Validated Assessment (r2), would you like us to also include pricing for the interim assessment (within the 3-year initial period noted in the ITN) which is required after 1 year of when the HITRUST certification is received?

A98. Yes

Q99. Will the interim assessment be included in the initial 3-year contract term?

A99. This is a topic for negotiation. The university is interested in maintaining the certification.

Q100. Should the pricing include the costs of the required HIPAA risk assessment or has this already been completed by the University?

A100. This is a topic for negotiation.

Q101. Would it be possible for references to be anonymized until bidders are shortlisted?

A101. Yes, but full details will be required during the negotiation phase

Q102. Does the University also want to attain CMMC certification?

A102. No

Q103. Are any significant changes, such as hardware upgrades or platform modifications, planned for 2022?

A103. No

Q104. Will a dedicated internal UF staff resource be assigned to facilitate the project?

A104. Yes

Q105. Are you planning to grant time extensions to respond to this RFP?

A105. At this point, no extension is planned. Any extensions will be communicated as an addendum and posted to the Procurement Services website.

Q106. Does the organization offer Infrastructure as a Service (IaaS)?

A106. HiPerGator is infrastructure for research and maps to PaaS and Saas.