Question Number	Page, Document, Section Reference, if applicalble	Questions	USHR Response
1	**Page 2 Hosting requirements**	Please share details regarding the on premise container orchestration platform.	Per Attachment J.10P the House operates an internal Kubernetes environment as a Container Orchestration Platform for hosting Contractor applications. See attachment J.10P for more details.
2	Page 3 Maintenance services	Please list the kind of hardware in scope for example Laptops, Desktops, mobile devices, printers, network switch etc	See §C.3.4.1, §C.3.4.5 (and subsections), and §C.3.5.2 (and subsections) for a description of hardware and responsibilities.
3	Page 3 Maintenance services	Is there any End of life and End of support hardware to be maintained? Are the systems patched and are current?	The House follows end of life and end of support dates provided by software providers and manufacturers. House office workstations and laptops are enrolled in an Enterprise patch-management program. See attachments J.4 and J.5 for support standards and requirements.
4	Page 3 Maintenance services	Is there an annual maintenenace contract in place?	No
5	Page 3 System Administration	How is the previllge access managed?	Technology Services Contract vendors manage their own company's Active Directory Organization Unit via a administrator group. OU administrators manage the creation, deletion, etc. of objects in their OU in accordance with House policies. Privileged account creation requirements are outlined in HISPOL 16 and related documents (available only to contracted vendors).
6	FedRAMP Requirements	Please confirm the specific FedRAMP authorization level (Low, Moderate, High) required for the "House Cloud Services Platform" and any related cloud-hosted components.	FedRAMP authorization is not required.
7	Cybersecurity & Information Security Compliance (C.6, H.14)	Could the House provide the detailed "House-defined timelines" for applying security patches and fixes, specifically for vulnerabilities classified as High, Medium, and Low severity?	Critical: within 72 hours* High: within 5 business days Medium/Low: within 30 days *time to remediate may be shorter depending on the vulnerability.
8	General Obligations	What are the "required House security and monitoring tools" that must be installed on contractor owned network connected devices, and what are the specific technical requirements for integrating vendor logs or monitoring output with House systems?	All contractor owned devices must be joined to the House domain, and be managed by the House. Once joined to the domain, House security and monitoring tools will be automatically installed. In accordance with House policies, users must ensure mobile and portable devices connected to the House network or with access to House information and information systems always have: • House-authorized MDM solutions installed and enabled. • House-designated mobile security applications installed and enabled. • Additional security features enabled on devices as prescribed by HIR.
9	Data Protection & Confidentiality Compliance (C.13, C.3.3.8, H.35)	Please define the House's specific requirements for the contents and format of the Data Escrow Agreement, particularly concerning the custody of "Admin passwords and encryption keys."	See §C.3.3.10 for escrow and content requirements.
10	Cybersecurity & Information Security Compliance	What is the formal process and criteria used by the House to determine a service poses a risk and must be disconnected or blocked, and what is the vendor's required notification and resolution timeline?	Determination of risk is at the discretion of the Cybersecurity Office. See §C.17(j) for security incident notificaation requirements.

11	Data Protection & Confidentiality Compliance (C.13)	Please clarify the scope and definition of "Client Data" and "Confidential Information." Does this term explicitly include any categories of Controlled Unclassified Information (CUI) or specific types of Personally Identifiable Information (PII) that require enhanced protection?	Yes.
12	Maintenance Services / Cloud & Hosting Compliance (C.3.3.5)	What is the House-approved method, standard, or tool required for the secure wiping of devices removed from service (Maintenance Services) and the verified destruction of House data on third-party cloud services (CMS)?	The CAO provides Microsoft DaRT DiskWipe for use by Maintenance Services contractors. Destruction of House data on externally hosted third-party services depends on the service. The Contractor must be able to provide verification of data destruction if requested by the CAO.
13	Data Protection & Confidentiality Compliance (C.13, H.35)	What are the mandatory "strict rules" and procedures for the contractor to follow when handling legal requests, such as subpoenas, for Client Data, including the required channel and timeline for House notification?	Requirements are specified in both sections C.13 and H.35.
14	Administrative & Contractual Compliance (H-clauses)	Does the mandatory Background Check requirement apply to all contractor personnel, or is it limited to those with privileged access to House systems or physical access to House facilities?	Background checks are required of all contractor personnel that perform work under the Technology Services Contract, or require access to the House network.
15	Systems Administration Services	Can the House specify the standard or framework (e.g., CIS Benchmarks, DISA STIGs) that defines the required "secure configurations" for servers, workstations, and network components?	Technical standards for server configurations and workstations, developed by the CAO, are made available to Contractors by the CAO.
16	Cybersecurity & Information Security Compliance (C.6, H.14)	Beyond the requirement to apply patches within "House-defined timelines," what is the current vulnerability severity matrix and the associated remediation SLA (Service Level Agreement) required for Critical, High, and Medium vulnerabilities?	Critical: within 72 hours* High: within 5 business days Medium/Low: within 30 days *time to remediate may be shorter depending on the vulnerability.
17	J.10G – HISPOL 17, Section 4.2; J.10N – House Cloud Services Platform	Can the HoR provide an updated list of authorized AWS cloud services available to CMS contractors on the House Cloud Services Platform? Specifically, is AWS Bedrock an authorized service, or can it be added to the list of approved services for use in supporting CMS capabilities?	A list of authorized AWS cloud services is not available. In accordance with §C.3.3(c) a House Information Security Policy 017.0 (HISPOL17) review is required for externally or cloud hosted services or applications and authorized for use (§C.3.2(f)). The House instance of AWS Bedrock may be considered for use by contractors.
18	General	Is there an expected award date?	Award dates may vary by vendor, and depend on type of service being provided, and complexity of CMS offeror's architecture and requirements.
19	General	How many vendors are currently performing the core tasks?	There are currently four (4) Correspondence Management System vendors, and five (5) Maintenance/Systems Administration vendor (including the CAO).