2026-001-049

Interpretations and Clarifications

5-14-26

Draft responses prepared from HACN RFP scope and available tenant/security reporting. Items requiring exact live tenant inventory should be validated during vendor discovery.

Shared mailboxes and Service Accounts; Do they 270 users referenced in the infrastructure scope cover the entirety of active mailboxes at HACN, or are there additional shared mailboxes, distribution lists, and unlicensed service accounts that also require threat inspection and protection?

Answer- For proposal purposes, vendors should price the managed email security solution for approximately 270 users. Shared mailboxes, service accounts, distribution groups, and other mail-enabled objects that require protection should be identified separately if the proposed platform licenses them differently.

Email Volume Metrics; What is the average monthly volume of email traffic (inbound and outbound messages) and what is the average volume of processed attachments across the organization?

Answer- Use the most recent available operational report as the current estimate: approximately 73,125 inbound emails and 13,614 outbound emails over the five-week reporting window. Attachment volume was not separately available from the reviewed tenant reports; vendors should identify any attachment-processing assumptions in their proposal.

Domain Coverage; How many active email domains does HACN currently operate that will need to be configured under the solutions DMARC, DKIM, SPF, anti-spoofing, and domain reputation protection policies?

Answer- For proposal purposes, vendors should assume HACN's primary production email domain is hacn.org. Any additional accepted or parked domains discovered during onboarding should be validated with HACN and included or priced separately if they materially affect scope.

Identity Security; should the licensing count for the Identity Security layer be strictly based on the 270 named users in Microsoft Entra ID, or are there active guests/third party accounts (B2B/Guest Accounts) that fall within the authentication rules?

Answer- Licensing should be based on approximately 270 named users for the base proposal. Active B2B/Guest accounts or third-party identities that are subject to authentication and monitoring policies should be identified separately during discovery and priced separately only if the vendor requires licensing for those accounts.

SIEM/ITSM Integration; is there a requirement for native SOC/ MDR integration with an existing SIEM (eg Microsoft Sentinel) or HACNs internal ticketing/ITSM platform for incident and ticket synchronization?

Answer- No external SIEM, SOAR, centralized syslog, or third-party SOC platform integration is mandatory for the base proposal unless the vendor's solution requires it. Integration with Microsoft 365, Exchange Online, Entra ID, Defender, and HACN notification/escalation workflows is required.

Can HACN confirm whether existing Microsoft Defender for Office 365 Pan 2 capabilities within the M365 E5 license should be directly managed and augmented by the vendor, or if HACN is seeking separate third-party API/MX security layer?

Answer- Seeking third-party API security layer

Regarding the preference for 24x7 SOC coverage, does HACN expect the vendors SOC to perform direct automated account containment and email quarantine, or act primarily in an advisory triage role with escalation to HACN IT?

Answer- The required managed monitoring is primarily focused on email-related security events and related identity/account-compromise signals connected to Microsoft 365, Exchange Online, Entra ID, and Defender. Broader endpoint, server, firewall, and network MDR may be proposed as optional but is not the primary base scope unless specifically listed.

What is the average monthly incoming and outgoing email volume across HACN’s `270 users and 23 office locations?

Answer- Use the most recent available operational report as the current estimate: approximately 73,125 inbound emails and 13,614 outbound emails over the five-week reporting window. Attachment volume was not separately available from the reviewed tenant reports; vendors should identify any attachment-processing assumptions in their proposal.

Are there specific Tribal sovereignty, FedRAMP, CJIS, or geographic data residency requirements governing where threat log telemetry and analytic data must be stored?

Answer- No additional FedRAMP, CJIS, geographic data residency, or tribal sovereignty requirement beyond applicable law and alignment with NIST Cybersecurity Framework has been identified in the reviewed materials. Vendors must disclose where data, logs, telemetry, and analyst work are stored and processed and identify any compliance limitations.

Can all project implementation, configuration assistance, administrator training, and ongoing managed SOC services be delivered 100% remotely?

Answer- Remote delivery is acceptable for implementation, configuration assistance, administrator training, and managed SOC services. Any requested onsite demonstrations or meetings should be clearly identified and priced separately.

Does HACN prefer an API- based post-delivery integration architecture via Microsoft Graph API or an inline mail flow (MX record/ MTA) Configuration?

Answer- HACN prefers an API-based integration model using Microsoft Graph and Microsoft 365 security signals where feasible to minimize mail-flow disruption. Inline MX/MTA architecture may be considered if the vendor explains the security benefit, operational impact, and rollback process.

Will the managed email security solution need to integrate with any external third party SIEM, SOAR, or centralized syslog infrastructure beyond the native M365/Defender ecosystem?

Answer- No external SIEM, SOAR, centralized syslog, or third-party SOC platform integration is mandatory for the base proposal unless the vendor's solution requires it.

Integration with Microsoft 365, Exchange Online, Entra ID, Defender, and HACN notification/escalation workflows is required.

For post-delivery automated remediation, does HACN require automated retraction for internal user-to-user emails in addition to external inbound emails?

Answer- Yes. The proposed solution should support post-delivery retraction/remediation for both external inbound messages and internal user-to-user messages when technically supported by Microsoft 365 and the vendor platform.

What are the specific Service Level Agreement (SLA) response time expectations for high severity incident escalations from the vendors SOC to the HACN designated personnel?

Answer- Critical: immediate notification, target initial escalation within 15 minutes. High: within 1 hour. Medium: same business day. Low: next business day. Final SLA language may be negotiated in the awarded agreement.

Does HACN currently utilize or plan to deploy third-party security awareness training or phishing simulation tools that must integrate with the proposed solution?

Answer- HACN uses user awareness and reporting processes and has referenced phishing campaigns and training as part of cybersecurity action planning. The proposed solution should support user-reported email workflows and should describe any security awareness or phishing simulation integrations if included.

What is the preferred initial contract term length (E.g. 1 year base with renewal options vs. 3 year multi year contract) for pricing structure?

Answer- HACN prefers a one-year base term with annual renewal options. Vendors may also provide optional multi-year pricing for comparison, subject to HACN approval and the non-appropriation clause.

On the Mandatory Response Sheet, what specific document format or proof is required for ‘Contracts/Agreements/ Support Assurances’?

Answer- Vendors should provide sample or proposed contract documents, support/SLA terms, service descriptions, escalation procedures, warranty or support assurances, and any required subscription or licensing agreements.

Will HACN afford vendors the opportunity to conduct a lice proof of concept or environment trial during the stage 1 review period prior to shortlisting top vendors?

Answer- HACN may consider vendor demonstrations, proof of concept activities, or limited trials during the review process when useful to validate fit. Any live environment access must be approved by HACN and performed under agreed security and confidentiality controls.

Should software licensing costs be quoted strictly on a fixed per-user per- month basis for ` 270 users, or should tiered user bands be provided?

Answer- Vendors should provide fixed per-user pricing for approximately 270 users and may include tiered pricing or optional pricing bands. Existing Microsoft licensing is HACN-provided and should be reused where applicable; vendors should only price incremental licensing required for their proposed solution.

Are there specific key personnel security certifications (CISSP, CCSP, Microsoft Certified Security Operations Analyst) required for the assigned SOC delivery team?

Answer- Relevant cybersecurity certifications should demonstrate the proposed team's security operations and Microsoft security competency. Examples include CISSP, CISM, CCSP, GIAC certifications, Microsoft Certified Security Operations Analyst, Microsoft 365 Security Administrator, or comparable certifications. HACN is not requiring one single certification if equivalent qualifications are clearly documented.

Is there a current incumbent provider providing the services requested in the RFP?

Answer- Yes. HACN currently uses Darktrace capabilities in the environment, including Darktrace Email, Network, and Identity coverage. This RFP is related to the expiring email security portion and the desire to evaluate managed email security options.

Can you confirm that servers and firewalls are out of scope for monitoring?

Answer- The base managed service should focus on email security and related Microsoft 365 identity/account-compromise signals. Broader IT environment monitoring for endpoints, servers, firewalls, or network infrastructure may be proposed as optional or future scope.

In terms of Threat Hunting, do you require proactive threat hunting, or reactive, as the result of a threat or threat indicator?

Answer- HACN prefers both proactive scheduled threat hunting and reactive threat hunting triggered by alerts, incidents, threat indicators, or Microsoft 365/Defender/Entra ID telemetry.

Can you provide details on your “existing security infrastructure” you require integration with?

Answer- Existing security infrastructure includes Microsoft 365 E5, Exchange Online, Microsoft Entra ID, Intune, Microsoft Defender/Defender for Office 365, Microsoft Defender XDR signals where applicable, Azure-hosted business application connectivity, and Darktrace Email/Network/Identity monitoring. HACN also has an internal IT help desk process; vendors should describe available ticketing or notification integrations.

Can you confirm that all users have a Microsoft 365 E5 license or are there some quantity with different licenses?

Answer- The RFP describes the current environment as Microsoft 365 E5 with Entra ID, Intune, and Defender. Vendors should assume the existing Microsoft security licensing remains HACN-provided and should identify any assumptions or additional licensing needed for their solution. 212 E5 licenses and 72 F3

HACNs environment description notes Microsoft 365 E5 licensing, which typically includes Microsoft Entra ID P2/ Identity Protection (impossible-travel and risky-sign-in detection). For the identity and account protection requirements in the Scope of Services, would HACN prefer the proposed solution to integrate with and act on those existing Entra ID

signals, or is HACN expecting the awarded solution to provide independent behavioral/anomaly detection outside of the Microsoft stack?

Answer- HACN prefers the selected solution to integrate with and act on existing Microsoft Entra ID / Identity Protection signals where possible. Vendors may include independent behavioral or anomaly detection if it adds value, but the proposal should avoid unnecessary duplication of existing Microsoft E5 capabilities.

Is Microsoft Defender for Office 365 currently licensed and active for the M365 environment? If so, should the proposed solution complement and run alongside existing Defender protections, or is Defender currently not being used for email security?

Answer- HACN expects vendors to maximize and complement the existing Microsoft investment, including Microsoft 365 E5, Exchange Online, Entra ID, Intune, Defender, and Defender for Office 365 capabilities. A third-party platform may be proposed if it provides clearly justified added value and does not create unnecessary duplicate licensing or administrative overhead.

Is there an incumbent vendor currently providing managed email security services to HACN? If so, what solution or services are currently in place?

Answer- Yes. HACN currently uses Darktrace capabilities in the environment, including Darktrace Email, Network, and Identity coverage. This RFP is related to the expiring email security portion and the desire to evaluate managed email security options.

What is HACNs anticipated project timeline, including the desired implementation start date and target go-live date?

Answer- HACN expects the selected vendor to provide a proposed implementation plan and timeline with milestones, required HACN resources, testing, administrator training, and production go-live activities. Final dates will be coordinated after award.

What is the estimated budget, budget range, or Not to Exceed amount allocated for this engagement, including licensing, implementation, and ongoing, managed services?

Answer- HACN is not publishing a target budget or not-to-exceed amount for this clarification. Vendors should submit their best-value proposal with transparent pricing for

licensing, implementation, managed services, professional services, and optional services.

What is the anticipated initial contract term and does HACN expect renewal options or a specific maximum contract duration?

Answer- HACN prefers a one-year base term with annual renewal options. Vendors may also provide optional multi-year pricing for comparison, subject to HACN approval and the non-appropriation clause.

Does HACN intend for the selected solution to replace any existing Microsoft Defender for Office 365 capabilities, or should it operate alongside and complement the existing Microsoft security stack?

Answer- HACN expects vendors to maximize and complement the existing Microsoft investment, including Microsoft 365 E5, Exchange Online, Entra ID, Intune, Defender, and Defender for Office 365 capabilities. A third-party platform may be proposed if it provides clearly justified added value and does not create unnecessary duplicate licensing or administrative overhead.

Are all approximately 270 users expected to be covered by the managed email security solution or are there additional shared mailboxes, service accounts, or other mail-enabled accounts, that should be included in licensing and pricing?

Answer- For proposal purposes, vendors should price the managed email security solution for approximately 270 users. Shared mailboxes, service accounts, distribution groups, and other mail-enabled objects that require protection should be identified separately if the proposed platform licenses them differently.

What level of authority will the selected vendor have to perform automated remediation actions, such as quarantining or retracting email and containing user accounts, without prior HACN approval?

Answer- Automated email actions such as quarantine, sender/domain blocking, URL blocking, and post-delivery message retraction may be performed under agreed playbooks. Higher-impact identity actions such as disabling accounts, forced password resets, or

broad containment should require HACN approval unless a specific emergency playbook is approved in advance.

What are HACNs required response and escalation SLAs for critical, high, medium, and low severity email security incidents?

Answer- Critical: immediate notification, target initial escalation within 15 minutes. High: within 1 hour. Medium: same business day. Low: next business day. Final SLA language may be negotiated in the awarded agreement.

Are there specific regulatory, data residency, data retention, or compliance requirements beyond alignment with the NIST Cybersecurity Framework that the proposed solution must satisfy?

Answer- No additional FedRAMP, CJIS, geographic data residency, or tribal sovereignty requirement beyond applicable law and alignment with NIST Cybersecurity Framework has been identified in the reviewed materials. Vendors must disclose where data, logs, telemetry, and analyst work are stored and processed and identify any compliance limitations.

Does HACN Require implementation, training, or ongoing support activities to be performed onsite or can these services be delivered remotely?

Answer- Remote delivery is acceptable for implementation, configuration assistance, administrator training, and managed SOC services. Any requested onsite demonstrations or meetings should be clearly identified and priced separately.

Expel can provide 24/7 MDR on technologies referenced in the RFP, and email security provided that there is a supported email tool in place (such as Mimecast, Sublime, Proofpoint, or Abnormal). Does HACN plan to produce one of these tools as part of this project?

Answer- The required managed monitoring is primarily focused on email-related security events and related identity/account-compromise signals connected to Microsoft 365, Exchange Online, Entra ID, and Defender. Broader endpoint, server, firewall, and network

MDR may be proposed as optional but is not the primary base scope unless specifically listed.

Do you have a preferred reseller/VAR that you work with so we can provide preliminary pricing? If not, we are happy to work with someone we recommend.

Answer- Our current reseller is Softchoice

Could the HACN please confirm whether this is a new initiative or an existing engagement?

Answer- Yes. HACN currently uses Darktrace capabilities in the environment, including Darktrace Email, Network, and Identity coverage. This RFP is related to the expiring email security portion and the desire to evaluate managed email security options.

Could the HACN provide the anticipated project timeline, including key milestones and the overall expected duration of the engagement?

Answer- HACN expects the selected vendor to provide a proposed implementation plan and timeline with milestones, required HACN resources, testing, administrator training, and production go-live activities. Final dates will be coordinated after award.

Could the HACN please clarify whether it intends to award this RFP to a single vendor or multiple vendors? If multiple awards are anticipated, could the HACN specify the expected number of vendors to be selected?

Answer- HACN intends to award to a single vendor for the managed email security solution unless Procurement determines that a different award structure is in HACN's best interest.

Please confirm whether all 270 users/mailboxes are expected to be covered by the proposed solution, or whether only a subset of users/mailboxes will be in scope.

Answer- For proposal purposes, vendors should price the managed email security solution for approximately 270 users. Shared mailboxes, service accounts, distribution groups, and other mail-enabled objects that require protection should be identified separately if the proposed platform licenses them differently.

Please provide the number of domains and email domains that will be protected under this engagement.

Answer- For proposal purposes, vendors should assume HACN's primary production email domain is hacn.org. Any additional accepted or parked domains discovered during onboarding should be validated with HACN and included or priced separately if they materially affect scope.

Are there any expected SLA requirements for alert triage, investigation, escalation, and incident notification that vendors should incorporate into pricing?

Answer- Critical: immediate notification, target initial escalation within 15 minutes. High: within 1 hour. Medium: same business day. Low: next business day. Final SLA language may be negotiated in the awarded agreement.

Please confirm whether HACN expects the proposed solution to replace, supplement, or operate alongside Microsoft Defender for Office 365 within the existing Microsoft 365 E5 Environment.

Answer- HACN expects vendors to maximize and complement the existing Microsoft investment, including Microsoft 365 E5, Exchange Online, Entra ID, Intune, Defender, and Defender for Office 365 capabilities. A third-party platform may be proposed if it provides clearly justified added value and does not create unnecessary duplicate licensing or administrative overhead.

Are there any existing email security, SIEM, SOC, SOAR, threat intelligence, or security monitoring platforms that the proposed solution will be required to integrate with?

Answer- No external SIEM, SOAR, centralized syslog, or third-party SOC platform integration is mandatory for the base proposal unless the vendor's solution requires it. Integration with Microsoft 365, Exchange Online, Entra ID, Defender, and HACN notification/escalation workflows is required.

Does HACN expect the selected vendor to perform the complete implementation and configuration including M365/Exchange Online/ Entra ID integration, policy configuration, testing, and production deployment?

Answer- Yes. HACN expects the selected vendor to provide complete implementation and configuration assistance, including Microsoft 365, Exchange Online, Entra ID, policy configuration, testing, validation, administrator training, documentation, and production deployment support.

To ensure accurate licensing and pricing, please provide the approximate monthly inbound and outbound email volume or average number of emails process per day?

Answer- Use the most recent available operational report as the current estimate: approximately 73,125 inbound emails and 13,614 outbound emails over the five-week reporting window. Attachment volume was not separately available from the reviewed tenant reports; vendors should identify any attachment-processing assumptions in their proposal.

Does HACN have historical data on the number of email security alerts/incidents per month that vendors should use for estimating managed service effort?

Answer- HACN has historical monthly security reporting that includes account-compromise alerts, DLP events, insider risk reviews, malware/virus activity, phishing attempts, user-reported emails, quarantine requests, and Darktrace/Microsoft Defender activity. Vendors should use those categories for estimating managed service effort and confirm any additional data required during discovery.

Are there any known budgetary constraints or target budget ranges that vendors should consider when developing their proposals?

Answer- HACN is not publishing a target budget or not-to-exceed amount for this clarification. Vendors should submit their best-value proposal with transparent pricing for licensing, implementation, managed services, professional services, and optional services.

Are there any on-site requirements for implementation, training, demonstrations, or ongoing service delivery that vendors should account for in their pricing?

Answer- Remote delivery is acceptable for implementation, configuration assistance, administrator training, and managed SOC services. Any requested onsite demonstrations or meetings should be clearly identified and priced separately.

Given HACNs existing Microsoft 365 E5, Microsoft Defender, and Entra ID environment, please clarify which capabilities HACN expects the selected vendor to provide through a third-party email security platform versus capabilities that may be provided through HACNs existing Microsoft security technologies.

Answer- HACN expects vendors to maximize and complement the existing Microsoft investment, including Microsoft 365 E5, Exchange Online, Entra ID, Intune, Defender, and Defender for Office 365 capabilities. A third-party platform may be proposed if it provides clearly justified added value and does not create unnecessary duplicate licensing or administrative overhead.

Please clarify whether the required 24x7 SOC monitoring and managed detection and response services are intended to be limited to email-related security events and threats, or whether HACN expects the vendor to monitor and respond to security events across the broader IT environment (e.g. endpoints, network, servers, and other security infrastructure).

Answer- The required managed monitoring is primarily focused on email-related security events and related identity/account-compromise signals connected to Microsoft 365, Exchange Online, Entra ID, and Defender. Broader endpoint, server, firewall, and network MDR may be proposed as optional but is not the primary base scope unless specifically listed.

What was the annual spend under the previous contract for these services?

Answer- HACN is not publishing prior annual spend through this clarification. Vendors should provide competitive pricing based on the published scope and their proposed solution.

If this is a new contract, what is the estimated annual budget?

Answer- HACN is not publishing a target budget or not-to-exceed amount for this clarification. Vendors should submit their best-value proposal with transparent pricing for licensing, implementation, managed services, professional services, and optional services.

Is the agency open to a hybrid delivery model utilizing a combination of onshore and offshore resources?

Answer- HACN prefers U.S.-based or clearly disclosed support resources. Vendors proposing offshore or hybrid support must identify the model, data access boundaries, security controls, and any data residency implications.

Will the work be performed onsite, remotely, or through a hybrid arrangement?

Answer- Remote delivery is acceptable for implementation, configuration assistance, administrator training, and managed SOC services. Any requested onsite demonstrations or meetings should be clearly identified and priced separately.

Would it be possible to consider a 1-2 week extension on the proposal submission deadline?

Answer- HACN is not granting a proposal deadline extension through this clarification unless separately posted by Procurement. Vendors should follow the published deadline and any formal addenda.

Are there any challenges, gaps, or pain points with the current solution or contractor that the agency is looking to address through this procurement?

Answer- Yes. HACN currently uses Darktrace capabilities in the environment, including Darktrace Email, Network, and Identity coverage. This RFP is related to the expiring email security portion and the desire to evaluate managed email security options.

Is there a projected contract award date and anticipated start date?

Answer- HACN has not published a separate projected award date or start date in this clarification. Vendors should follow the RFP review cycle and provide an implementation timeline that can begin after award and purchase authorization.

Are there any mandatory subcontracting goals associated with this contract?

Answer- No mandatory subcontracting goals are identified in this clarification. Cherokee/Indian preference and TERO certification requirements remain applicable as stated in the RFP.

Does HACN plan to keep Microsoft Defender for 365/Defender CDR as its primary email security platform or are you open to adding or replacing it with another solution?

Answer- HACN expects vendors to maximize and complement the existing Microsoft investment, including Microsoft 365 E5, Exchange Online, Entra ID, Intune, Defender, and Defender for Office 365 capabilities. A third-party platform may be proposed if it provides clearly justified added value and does not create unnecessary duplicate licensing or administrative overhead.

Does HACN currently use Microsoft Sentinel or another SIEM? If so, would you like the proposed solution to integrate with it?

Answer- No external SIEM, SOAR, centralized syslog, or third-party SOC platform integration is mandatory for the base proposal unless the vendor's solution requires it. Integration with Microsoft 365, Exchange Online, Entra ID, Defender, and HACN notification/escalation workflows is required.

Can vendors propose a solution that uses both a technology provider and a separate managed security /MDR provider?

Answer- Yes. Vendors may propose a solution that combines a technology provider and a separate managed security/MDR provider, provided the proposal clearly identifies roles, responsibilities, escalation ownership, support model, and pricing.

For automated response, can actions be handled across Defender XDR, Entra ID, and another email security solution or does HACN want those capabilities provided by a single platform?

Answer- Automated email actions such as quarantine, sender/domain blocking, URL blocking, and post-delivery message retraction may be performed under agreed playbooks. Higher-impact identity actions such as disabling accounts, forced password resets, or broad containment should require HACN approval unless a specific emergency playbook is approved in advance.

For QR code threat detection, does that capability need to be native to the email security platform, or can it be provided through an integrated solution?

Answer- QR-code threat detection may be native to the email security platform or delivered through an integrated solution, provided the vendor explains how it detects, blocks, reports, and remediates QR-code based threats.

What level of automated Entra ID account response is HACN looking for? For example, session revocation, disabling accounts, or password resets.

Answer- HACN is interested in account response capabilities such as session revocation, password reset initiation, and disabling accounts, but these actions should be governed by approved playbooks and HACN approval for high-impact actions unless emergency authority is separately granted.

Are there any additional regulatory or compliance requirements, such as HUD or tribal requirements, that vendors should account for in their response?

Answer- No additional FedRAMP, CJIS, geographic data residency, or tribal sovereignty requirement beyond applicable law and alignment with NIST Cybersecurity Framework has been identified in the reviewed materials. Vendors must disclose where data, logs, telemetry, and analyst work are stored and processed and identify any compliance limitations.

Microsoft Defender for Office 365: Please confirm whether Defender for Office 365 is currently enabled and actively configured. Additionally, does HACN prefer the selected

vendor to manage and enhance the existing Microsoft-native email security capabilities, or is HACN open to an additional email security platform where technically justified?

Answer- HACN expects vendors to maximize and complement the existing Microsoft investment, including Microsoft 365 E5, Exchange Online, Entra ID, Intune, Defender, and Defender for Office 365 capabilities. A third-party platform may be proposed if it provides clearly justified added value and does not create unnecessary duplicate licensing or administrative overhead.

Mailbox Count and Tenant Structure: Please confirm the approximate number of mailboxes requiring protection, including user, shared, service, and other non-user mailboxes. Are all applicable mailboxes contained within a single Microsoft 365 tenant?

Answer- For proposal purposes, vendors should price the managed email security solution for approximately 270 users. Shared mailboxes, service accounts, distribution groups, and other mail-enabled objects that require protection should be identified separately if the proposed platform licenses them differently.

Existing Security Infrastructure: The RFP requires integration with HACN's "existing security infrastructure." Please identify any existing SIEM, SOC platform, security orchestration platform, or IT service management/ticketing system with which email security alerts or incidents are expected to integrate.

Answer- No external SIEM, SOAR, centralized syslog, or third-party SOC platform integration is mandatory for the base proposal unless the vendor's solution requires it. Integration with Microsoft 365, Exchange Online, Entra ID, Defender, and HACN notification/escalation workflows is required.

Existing Microsoft Licensing: Please confirm whether HACN's existing Microsoft 365 E5, Defender, Entra ID, and related Microsoft licensing will remain HACN-provided throughout the engagement, with vendors expected to price only incremental licensing required for their proposed solution.

Answer- The RFP describes the current environment as Microsoft 365 E5 with Entra ID, Intune, and Defender. Vendors should assume the existing Microsoft security licensing remains HACN-provided and should identify any assumptions or additional licensing needed for their solution.

Contract/Subscription Term: Please identify the desired initial contract or subscription term for pricing purposes. Would HACN like vendors to provide both one-year and multi-year pricing options?

Answer- HACN prefers a one-year base term with annual renewal options. Vendors may also provide optional multi-year pricing for comparison, subject to HACN approval and the non-appropriation clause.

Implementation Timeline: Does HACN have a target production go-live date or preferred implementation window following contract award?

Answer- HACN expects the selected vendor to provide a proposed implementation plan and timeline with milestones, required HACN resources, testing, administrator training, and production go-live activities. Final dates will be coordinated after award.

The RFP states approximately 270 users and 1,000 devices. Can HACN provide a detailed asset inventory, including:

o User counts by type (employees, contractors, shared mailboxes)

o Number of mailboxes 285

o Endpoints 268 Windows devices

o Servers de

o Service accounts de

o Privileged accounts de

o Distribution lists and shared mailboxes? 29

Can HACN provide current Microsoft 365 tenant details, including:

o Number of licensed users 270 E5 users, 72 F3 users

o Number of active mailboxes 285

o Number of inactive/shared mailboxes? 29

The RFP references Microsoft 365 (E5), Entra ID, Intune, and Defender. Can HACN confirm the exact Microsoft licensing currently deployed across the environment?

Answer- The RFP describes the current environment as Microsoft 365 E5 with Entra ID, Intune, and Defender. Vendors should assume the existing Microsoft security licensing remains HACN-provided and should identify any assumptions or additional licensing needed for their solution.

Are all users licensed with Microsoft 365 E5, or is there a mix of licensing tiers (e.g., E3, E5, G3, G5, G5 Security, Frontline, etc.)?

Answer- The RFP describes the current environment as Microsoft 365 E5 with Entra ID, Intune, and Defender. Vendors should assume the existing Microsoft security licensing remains HACN-provided and should identify any assumptions or additional licensing needed for their solution.

Are there any plans to upgrade, downgrade, or change Microsoft licensing tiers in the foreseeable future?

Answer- The RFP describes the current environment as Microsoft 365 E5 with Entra ID, Intune, and Defender. Vendors should assume the existing Microsoft security licensing remains HACN-provided and should identify any assumptions or additional licensing needed for their solution.

Can HACN provide details of any existing email security, anti-phishing, or managed detection services currently in use?

Answer- HACN currently uses Microsoft Defender/Defender for Office 365 capabilities and Darktrace Email, with Darktrace Network and Identity also configured. Vendors should leverage existing Microsoft investments where possible and clearly describe any proposed third-party email security platform.

Is HACN seeking a fully managed email security platform with managed services, or enhancement of existing Microsoft security controls and investments?

Answer- HACN is seeking a managed email security solution that can either enhance the existing Microsoft security controls or include incremental technology where justified. Proposals should clearly separate Microsoft-native service management from any added third-party platform licensing.

Are there any specific email security technologies, vendors, or platforms that HACN prefers vendors to leverage, considering the RFP states a preference for maximizing existing Microsoft investments?

Answer- HACN currently uses Microsoft Defender/Defender for Office 365 capabilities and Darktrace Email, with Darktrace Network and Identity also configured. Vendors should leverage existing Microsoft investments where possible and clearly describe any proposed third-party email security platform.

The RFP requires continuous monitoring and references 24x7 monitoring and expert analysis. Can HACN confirm whether 24x7 monitoring coverage is a mandatory requirement or a preferred capability?

Answer- 24x7 monitoring and expert analysis are a preferred and important evaluation capability. Vendors should clearly state whether 24x7 SOC coverage is included in the base proposal, optional, or not available.

Does HACN require monitoring exclusively for email security events, or should monitoring include related identity-based threats detected through Microsoft Entra ID integration?

Answer- Monitoring should include email security events and related identity-based threats detected through Microsoft Entra ID, Defender, and Microsoft 365 signals. Broader

endpoint, server, firewall, or network monitoring may be proposed as optional or future scope unless explicitly included by the vendor.

Does HACN require a dedicated SOC team, named analysts, or is a shared SOC model acceptable?

Answer- A shared SOC model is acceptable if coverage, escalation, accountability, and reporting meet HACN requirements. Vendors should identify whether named analysts, dedicated resources, or a shared SOC will be used.

What are the expected notification and escalation timelines for critical email security incidents?

Answer- Critical: immediate notification, target initial escalation within 15 minutes. High: within 1 hour. Medium: same business day. Low: next business day. Final SLA language may be negotiated in the awarded agreement.

Does HACN require the selected provider to perform active incident response actions on behalf of HACN, or only provide investigation findings and response recommendations?

Answer- Automated email actions such as quarantine, sender/domain blocking, URL blocking, and post-delivery message retraction may be performed under agreed playbooks. Higher-impact identity actions such as disabling accounts, forced password resets, or broad containment should require HACN approval unless a specific emergency playbook is approved in advance.

For automated response capabilities such as quarantine, message retraction, user containment, and blocking actions, should these actions be performed automatically or require HACN approval before execution?

Answer- Automated email actions such as quarantine, sender/domain blocking, URL blocking, and post-delivery message retraction may be performed under agreed playbooks. Higher-impact identity actions such as disabling accounts, forced password resets, or broad containment should require HACN approval unless a specific emergency playbook is approved in advance.

Does HACN expect the vendor to perform containment and remediation activities during non-business hours, weekends, and holidays?

Answer- For critical email security incidents, HACN expects the vendor to monitor and escalate outside normal business hours, including weekends and holidays. Actual remediation authority should follow the approved response playbooks.

Can HACN clarify the escalation matrix, roles, and points of contact for security incidents

Answer- The escalation matrix and designated points of contact will be finalized during onboarding. Vendors should provide a recommended escalation model and list required HACN roles during implementation.

The RFP includes threat hunting activities. Does HACN expect proactive scheduled threat hunting activities, or threat hunting only when alerts or incidents occur?

Answer- HACN prefers both proactive scheduled threat hunting and reactive threat hunting triggered by alerts, incidents, threat indicators, or Microsoft 365/Defender/Entra ID telemetry.

Does HACN require investigation of historical email activity as part of incident response and threat hunting activities?

Answer- HACN prefers both proactive scheduled threat hunting and reactive threat hunting triggered by alerts, incidents, threat indicators, or Microsoft 365/Defender/Entra ID telemetry.

Does HACN have any specific retention requirements for operational reports, dashboards, and historical threat data?

Answer- HACN expects operational dashboards, daily/weekly threat summaries where available, monthly executive summary reporting, incident summaries, alert statistics, threat trends, key risk indicators, recommendations, and exportable historical reporting.

Are there any required report formats, executive reporting templates, or compliance reporting requirements that must be supported?

Answer- HACN expects operational dashboards, daily/weekly threat summaries where available, monthly executive summary reporting, incident summaries, alert statistics, threat trends, key risk indicators, recommendations, and exportable historical reporting.

Beyond Microsoft 365, Exchange Online, Entra ID, and Microsoft Defender, are there any additional security platforms, SIEM platforms, ticketing systems, or ITSM tools that require integration?

Answer- No external SIEM, SOAR, centralized syslog, or third-party SOC platform integration is mandatory for the base proposal unless the vendor's solution requires it. Integration with Microsoft 365, Exchange Online, Entra ID, Defender, and HACN notification/escalation workflows is required.

Can HACN provide details regarding the "existing security infrastructure" referenced in the RFP for integration planning purposes?

Answer- Existing security infrastructure includes Microsoft 365 E5, Exchange Online, Microsoft Entra ID, Intune, Microsoft Defender/Defender for Office 365, Microsoft Defender XDR signals where applicable, Azure-hosted business application connectivity, and Darktrace Email/Network/Identity monitoring. HACN also has an internal IT help desk process; vendors should describe available ticketing or notification integrations.

Does HACN have a target implementation timeline or desired go-live date for the managed email security service?

Answer- HACN expects the selected vendor to provide a proposed implementation plan and timeline with milestones, required HACN resources, testing, administrator training, and production go-live activities. Final dates will be coordinated after award.

Are there any implementation blackout periods, change-management restrictions, or business-critical dates that could impact deployment planning?

Answer- No specific implementation blackout periods are identified in this clarification. Vendors should propose a change plan that accommodates HACN maintenance windows, business-critical dates, and standard approval processes.

How many administrators will require training and knowledge-transfer sessions?

Answer- Vendors should plan administrator training and knowledge transfer for the HACN IT/security administrators who will manage or review the solution. For pricing, assume a small administrator group and include options for additional sessions if needed.

Following implementation, what support model does HACN expect from the selected vendor:

· Business-hours support

· Extended-hours support

· 24x7 support? 24/7

Does HACN require the vendor to provide ongoing platform administration, health monitoring, tuning, and policy optimization after deployment?

Answer- Following implementation, HACN expects ongoing platform administration, health monitoring, tuning, policy optimization, reporting, and support. Vendors should include 24x7 security escalation for critical incidents and describe business-hours versus extended-hours support for normal requests.

Are there any specific service level expectations for incident response, support requests, or issue resolution that vendors should incorporate into their proposals?

Answer- Critical: immediate notification, target initial escalation within 15 minutes. High: within 1 hour. Medium: same business day. Low: next business day. Final SLA language may be negotiated in the awarded agreement.

The pricing section references licensing, managed services, implementation services, professional services, and optional services. Can HACN confirm whether all licensing should be included in the proposal pricing, or whether any existing licenses will be reused?

Answer- Vendors should provide fixed per-user pricing for approximately 270 users and may include tiered pricing or optional pricing bands. Existing Microsoft licensing is HACN-provided and should be reused where applicable; vendors should only price incremental licensing required for their proposed solution.

Does HACN expect vendors to propose a complete managed email security solution inclusive of software licensing and managed services, or managed services leveraging existing Microsoft licensing investments where possible?

Answer- The RFP describes the current environment as Microsoft 365 E5 with Entra ID, Intune, and Defender. Vendors should assume the existing Microsoft security licensing remains HACN-provided and should identify any assumptions or additional licensing needed for their solution.

Are there any budgetary constraints or preferred commercial models (annual subscription, multiyear agreement, per-user licensing, etc.) that vendors should consider when preparing pricing?

Answer- HACN prefers a one-year base term with annual renewal options. Vendors may also provide optional multi-year pricing for comparison, subject to HACN approval and the non-appropriation clause.

Please clarify what is required in Relevant cybersecurity certifications?

Answer- Relevant cybersecurity certifications should demonstrate the proposed team's security operations and Microsoft security competency. Examples include CISSP, CISM, CCSP, GIAC certifications, Microsoft Certified Security Operations Analyst, Microsoft 365 Security Administrator, or comparable certifications. HACN is not requiring one single certification if equivalent qualifications are clearly documented.

Please clarify what is required in Proof of professional licenses which are required with the proposal?

Answer- Proof of professional licenses means copies or documentation of any licenses, registrations, certifications, partner authorizations, or regulatory credentials required by law or required to deliver the proposed services. If no professional license is legally required for the proposed work, vendors should state that and provide applicable cybersecurity certifications and company credentials.