2025 Comprehensive Cybersecurity Assessment and Services Response to Inquiries

Question	Response
Can you please elaborate on the current systems and/or software that have been implemented for SBCERA?	Details of our current systems and software will be disclosed with the vendor after they are selected and a confidentiallity agreement is signed.
infrastructure, including the number of routers, switches, access points, firewalls, servers, etc.?	points, firewalls, servers, etc. Additional detail to be provided to selected vendor after confidentiality agreement is signed.
Do you require onsite support or open for Hybrid model?	be presented to our board members in person at the conclusion of the audit and its related activity.
How many employees do you currently have?	We have fewer than 100 employees.
their name?	We do not have an incumbent provider at this time.
Do you have a specified budget for this RFP? If so, could you please let us know?	organization's budget and needs. Our fiduciary responsibility is always considered, but it is not the only major factor considered when assessing security products and services.
How many Applications & Web Applications that need to be tested	This can range between 3 -5 applications, but may increase if including cloud applications, depending on definition of scope.
will participate? How many training sessions will you need each month?	training. Training options can be included in the proposal as a value-added service for consideration.
Has SBCERA formally adopted a security framework for its security program? If so, which one?	We attempt to follow NIST frameworks, but hope the selected partner can help determine the framework which best applies to our organization.
Does SBCERA have a formally established program to ensure compliance with cybersecurity and/or privacy regulations to which it is subject? If so, which regulations does it apply to?	adhere to multiple framework and legislative principles, including, but not limited to, CSF, 800-53, 800-171, GDPR, HIPPA, etc. We expect the selected cybersecurity audit services partner will be able to help us better determine and narrow down what framework(s) applies best and what regulation we must truly
assessments, please provide the following information (or estimates) as you are able:	points, firewalls, servers, etc. Additional detail to be provided to selected vendor after confidentiality agreement is signed.
· Number of devices to be reviewed	devices.
· Number of applications/systems to be reviewed	Dependiing on definition, this could range anywhere from 2 - 30, possibly more.
· Number of network infrastructure devices, including firewalls and similar security devices to be reviewed	points, firewalls, servers, etc. Additional detail to be provided to selected vendor after confidentiality agreement is signed.
· Number of physical locations for wireless assessment	assessment.
cloud usage?	Our usage is hybrid, with mostly SaaS and some PaaS applications.

Does SBCERA have a formal data classification policy and associated inventory of sensitive data?	objective and the expectation is the selected vendor will assist through consulting.
Can you provide any detail on the current usage of AI systems?	Currently, Most usage stems from generative AI for general tasks.
Does SBCERA currently use any commercial software or services for security awareness training or phishing simulation?	Yes, we are currently using a provider to facillitate security awareness training and phishing simulations.
Number of internal and external IPs in scope	points, firewalls, servers, etc. Additional detail to be provided to selected vendor after confidentiality agreement is signed.
Number of dynamic pages and user roles for web application testing	medium dynamic page density up to 100 pages, and 1-2 applications with high dynamic page density up to 200 pages.
Size of the organization (approximate number of employees)	We have fewer than 100 employees.
Number of locations and departments	assessment.
Hybrid)	Our usage is hybrid, with mostly SaaS and some PaaS applications.
Number of SSIDs to be assessed	We have less than 10 SSIDs.
Cloud platform in scope (e.g., AWS, Azure, GCP)	details will be provided to selected vendor upon signing of confidentiality agreement.
Number of cloud services currently in use	We have less than 30 cloud services in use.
Number of cloud accounts in scope	but we estimate no more than 35.
Number of domains to be included in the exercise	Only 1 domain will be included in this exercise.
Number of code repositories to be assessed	Source code not likely to be included as it is owned by the software developer.
external hosts) does SBCERA have that would be included in this testing?	points, firewalls, servers, etc. Additional detail to be provided to selected vendor after confidentiality agreement is signed.
internal hosts) does SBCERA have that would be included in this testing?	points, firewalls, servers, etc. Additional detail to be provided to selected vendor after confidentiality agreement is signed.
Can a breakdown of the total number of internal in use IP addresses be given detailing approximately how many servers, desktops, networking devices, IoT devices etc are in this figure?	For bidding purposes this info will be generalized. Detailed information will be provided with selected partner after confidentiality agreement is signed.
How many windows domains are in use at SBCERA?	Only 1 domain will be included in this exercise.
tested in order to give SBCERA sufficient internal network testing coverage (for example, IT and OT networks are typically segmented, preventing network connectivity between the two and requiring that testing be conducted from both perspectives in order to achieve full coverage)?	We would expect all internal and external systems to be audited, including cloud systems where applicable.
How many web applications are in use across SBCERA networks?	This can range between 3 -5 applications, but may increase if including cloud applications, depending on definition of scope.
products?	and internally developed.

How many home-grown/custom (in-house developed) web applications are in use at SBCERA?	We utilize a mixture of both off the shelf and custom products, both externally and internally developed.
for SBCERA web applications or will standard unauthenticated blackbox testing of these be sufficient? If more in-depth testing is desired, please describe the number of web applications that would be subject to this testing, along with how many user roles are available on these applications and any other markers that could be used to gauge the overall complexity of those	We would expect all internal and external systems to be thoroughly audited, including cloud systems where applicable.
the SBCERA, and how many physical locations are these SSIDs spread between?	We have less than 10 SSIDs in use.
How many AI models are in use that need to be tested for biases, adversarial risks, and model exploits?	None at this time.
What cloud environments are in use at SBCERA?	details will be provided to selected vendor upon signing of confidentiality agreement.
Approximately how many storage buckets are in use across SBCERA's cloud infrastructure?	For bidding purposes this info will not be disclosed. Detailed information will be provided with selected partner after confidentiality agreement is signed.
Approximately how many compute nodes are in use across SBCERA's cloud infrastructure?	For bidding purposes this info will not be disclosed. Detailed information will be provided with selected partner after confidentiality agreement is signed.
Approximately how many networks are in use across SBCERA's cloud infrastructure?	For bidding purposes this info will not be disclosed. Detailed information will be provided with selected partner after confidentiality agreement is signed.
Approximately how many databases are in use across SBCERA's cloud infrastructure?	For bidding purposes this info will not be disclosed. Detailed information will be provided with selected partner after confidentiality agreement is signed.
Approximately how many microservices are in use across SBCERA's cloud infrastructure?	For bidding purposes this info will not be disclosed. Detailed information will be provided with selected partner after confidentiality agreement is signed.
Approximately how many projects/accounts are in use across SBCERA's cloud infrastructure?	For bidding purposes this info will not be disclosed. Detailed information will be provided with selected partner after confidentiality agreement is signed.
Could you please provide External: Number of IPs/assets and frequency of testing.	provided with selected partner after confidentiality agreement is signed. In total, we have less then 500 devices, and expect yearly testing.
Could you please provide Internal: Number of IPs/assets and frequency of testing.	provided with selected partner after confidentiality agreement is signed. In total, we have less then 500 devices, and expect yearly testing.
Could you please provide Web Applications: Number and frequency of testing.	This can range between 3 -5 applications, but may increase if including cloud applications, depending on definition of scope. All testing would be yearly.
Could you please provide Are mobile applications included in the scope? If yes, number and frequency.	Mobile applications will not be included in scope.
and frequency.	API testing will likely not be included in scope.

Could you please specify The number and types of network devices in scope.	points, firewalls, servers, etc. Additional detail to be provided to selected vendor after confidentiality agreement is signed.
Could you please specify The number and types of security devices in scope.	points, firewalls, servers, etc. Additional detail to be provided to selected vendor after confidentiality agreement is signed.
Could you please specify Whether configuration reviews are part of the assessment scope.	We would expect all internal and external systems to be audited, including configurations where applicable.
Could you please confirm The total number of employees for social engineering testing.	We have fewer than 100 employees that would be subject to testing.
Could you please confirm The specific scenarios for social engineering campaigns you would like to include.	This would be based on the selected vendor's recommendation and current best practices.
Could you please clarify The number of regions/offices in scope.	assessment.
APIs.	We have less than 10 SSIDs in use.
Could you please confirm The cloud service provider(s) being used.	For bidding purposes this info will not be disclosed. Detailed information will be provided with selected partner after confidentiality agreement is signed.
Could you please confirm Whether configuration reviews of cloud infrastructure, OS, and DB instances are included in the scope.	We would expect all internal and external systems to be audited, including configurations where applicable.
scope.	critical systems where applicable.
Could you please provide Any reference or framework being used for internal control review.	We attempt to follow NIST frameworks, but hope the selected partner can help determine the framework which best applies to our organization.
scope?	No, AI or ML applications in scope at this time.
Could you please confirm Whether a Blue Team is in place at SBCERA for collaborative exercises.	We do not have a blue team in place at this time, but expect the selected partner to help develop and to collaborate with us.
Could you please confirm Our Red Team will conduct collaborative security exercises, attack simulations, reporting, and training.	Yes, this expected but likely at a later date and not during initial exercises.
Could you please confirm Can we use a “live-fire” approach (Red Team openly informs Blue Team after each simulated attack)?	This would be based on the selected vendor's recommendation and current best practices.
Could you please provide details on The development framework(s) currently being used.	Our approach varies based on the project tackled, but we tend to work in an iterative fashion.
team involved.	The development team is composed of less then 10 personnel.
agreement with SBCERA?	Our CIO and/or CEO would be those with authority to sign an agreement.
Are there specific preferences or constraints for negotiating arrangements regarding on-premises and remote work?	be presented to our board members in person at the conclusion of the audit and its related activity.
Could you provide examples of acceptable formats or templates for the detailed audit plan?	should be detailed enough to thoroughly understand scope, objective, prerequisities, actions, expected outcomes, and timelines. Bullet points should be used to summarize and the documentation should be in word or pdf format.

How often should periodic updates on the audit process be provided, and what level of detail is expected?	Weekly updates should suffice. However, critical findings should be communicated to CISO/ and or Security Manager as soon as possible.
Are there particular NIST frameworks that should be prioritized during the evaluation?	adhere to multiple framework and legislative principles, including, but not limited to, CSF, 800-53, 800-171, GDPR, HIPPA, etc. We expect the selected cybersecurity audit services partner will be able to help us better determine and narrow down what framework(s) applies best and what regulation we must truly
Could you clarify which compliance regulations (e.g., GDPR, HIPAA, ISO 27001) are most critical for the organization?	nature of our organization and industry, we do need to consider GDPR, HIPPA, etc. We expect our selected vendor will be able to help us confirm what regulatory legislation we must follow.
What is the preferred structure and format for the compliance roadmap?	enough to understand the tasks, milestones, and objectives, etc. required to achieve our compliance goals.
Are there current governance frameworks in place, or will the assessment involve building them from scratch?	adhere to multiple framework and legislative principles, including, but not limited to, CSF, 800-53, 800-171, GDPR, HIPPA, etc. We expect the selected cybersecurity audit services partner will be able to help us better determine and narrow down what framework(s) applies best and what regulation we must truly
Are there particular external or internal systems that should be prioritized during penetration testing?	Yes, there should be a focus on our pension administration system as well as our edge and perimeter systems.
Should phishing simulations target specific user groups or departments within the organization?	This would be based on the selected vendor's recommendation and current best practices.
assessments that the	
What metrics or reports are required to evaluate the effectiveness of incident response and disaster recovery plans?	factors, but this would require further discussion with our selected vendor to determine other data points to evaluate.
Are there predefined categories for sensitive data classification, or is this expected to be developed during the evaluation?	objective and the expectation is the selected vendor will assist through consulting.
Could you confirm which encryption protocols and algorithms (e.g., AES-256, TLS) are mandatory or preferred?	We prefer to adopt the strongest and most stable protocols and algorithms, while considering post-quantum ramifications.
What retention period is required for data deletion policies, and are there specific secure methods that must be implemented?	Retention is currently based on legal requirements and thus varies. Destruction methods are identified in our retention policy.
assessed?	No, not at this time.
Does the organization have established AI governance frameworks, or will these need to be developed?	An AI governance policy was passed and adopted recently. That said, review of the policy may be included as part of our overall review.
Could you clarify the priority areas for ethical AI practices, such as bias detection or adversarial risks?	There are no priority areas for AI at this time.
Are there specific real-world scenarios or attack simulations that the Purple test exercise should focus on?	This would be based on the selected vendor's recommendation and current best practices.

effectiveness of security monitoring during the Purple Team exercise?	notifications we would expect, in addition to any other data points recommended by vendor.
Should updated reports provide additional information on the root causes of unresolved vulnerabilities?	Yes, any additional information should be included.
What is the expected frequency and scope for tabletop exercises or incident response readiness assessments?	start at a later date after the initial assessment and engagement with our selected vendor.
Are there preferred methods or tools for policy and procedure development to ensure compliance with standards?	We do not have a preferred method or tool for policy and procedure development to ensure compliance with standards at this time.
Can you clarify if there are specific areas within the scope that are a priority (e.g., penetration testing, compliance assessment)?	We expect all systems, internal, external, on-premises and cloud-based to to be audited with a focus on penetration, compliance, and risk.
Are there any services or deliverables outside the stated scope that may be included later during the engagement?	No, not at this time.
Which departments or teams will be directly involved in or impacted by the audit and assessment process?	The Information Systems department will be primarily involved, though the assessment process will likely impact every department.
Will training programs and awareness sessions target all departments, or are specific teams prioritized?	Our entire organization is subject to security awareness training and simulation testing.
Could you provide an inventory or overview of the assets that fall within the scope (e.g., servers, network devices, endpoints)?	points, firewalls, servers, etc. Additional detail to be provided to selected vendor after confidentiality agreement is signed.
Are there critical assets or systems with unique security requirements or configurations?	No, most will be configured on best practice at the time it was configured.
should consider while designing solutions or conducting assessments?	purposes, no. We will consider our selected vendor's recommendations and current best practice at the point in time.