NIST Cybersecurity Framework		
Function	**Category**	**Questions**
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the entity to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the entity's risks Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the entity to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the entity's risk strategy.	Does the organization develop and documents policy for an inventory of information system components?
		Does the organization develop and documents policy for an inventory of information system components?
		Are there procedures in place for physical device inventory?
		Is system inventory documented such that the following requirements is met: It accurately reflect the current information system?
		Does The organization employ automated mechanisms to update physical device inventory?
		Does the organization develop and documents policy for software platform and application inventory?
		Does the organization develop and documents policy for software platform and application inventory?
		Is system inventory for software platform and application documented such that the following requirements is met: It accurately reflect the current information system?
		Does the information system provide the least functionality to meet operational needs?
		Does the organization perform all the following requirements: Identify software programs not authorized to execute on the information system? Employ a deny-all, allow by exception policy to prohibit the execution of unauthorized software on the information system? Review and update a list of unauthorized software programs?
		Is the information and information system categorized following FIPS 199-200, and NIST 800-53 requirements?
		Does the organization have documented procedures for how to categorize information systems?
		Does the organization have documented system categorization for mission critical systems (tested via relevant sample) or a documented decision to apply "Moderate" categorization for all systems?
		Do All information systems have documented system categorization per FIPS 199? Provide Tested via relevant sample.
		Is the security categorization decision per FIPS 199 reviewed and approved by the authorizing official or authorizing official designated representative?
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and	Does the Entity have a BIA and a TRP?
		Does the organization conduct annual Business Impact Analysis (BIA) for the system?
		Does Entity have a TRP which was informed from a Business Impact Analysis (BIA)?
		Does the organization identify critical information system assets supporting essential missions and business functions?

IDENTIFY (ID)	prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	Do you perform contingency plan or disaster recovery testing to test the execution of the contingency plan? Provide the results or reports from all contingency plan testing which have taken place since the last assessment which included testing TRP?
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the entity's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	Has a Privacy Impact Assessment (PIA) been conducted for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, or any existing organizational policies and procedures?
		Has a Privacy Impact Assessment (PIA) been conducted for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, or any existing organizational policies and procedures?
		Are sufficient resources allocated (organization-defined allocation of budget and staffing) to implement and operate the organization-wide privacy program?
		Are sufficient resources allocated (organization-defined allocation of budget and staffing) to implement and operate the organization-wide privacy program? Is a risk management process documented and implemented along with Privacy Impact Assessment (PIA)?
		Are privacy plans, policies, and procedures updated according to the organization-defined frequency, at least annually?
		Has a strategic organizational privacy plan been developed for implementing applicable privacy controls, policies, and procedures? For publicly accessible content, have designated individuals been authorized to post information onto a publicly accessible information system?
		Has a strategic organizational privacy plan been developed for implementing applicable privacy controls, policies, and procedures? For publicly accessible content, have designated individuals been authorized to post information onto a publicly accessible information system?
		Is effective notice provided to the public and to individuals regarding? or Provide evidence demonstrating effective notice to the public and to individuals that states the following: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII); (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary.
		For publicly accessible content, have designated individuals been authorized to post information onto a publicly accessible information system?
		Are public notices revised to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change?

IDENTIFY (ID)		Does the organization develop and disseminates an organization-wide information security program plan Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the nation associated with the operation and use of information system?
		Does the organization develop and disseminate an organization-wide information security program plan and develop a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the nation associated with the operation and use of information system?
		Does the organization review and update the risk management strategy at least quarterly to [discuss, prioritize, address, and monitor identified risks, including security risks.] or as required, to address organizational changes?
		Does the organization measure the effectiveness of its information security program with Key Performance Indicators (KPIs)?
		Does the organization develop, monitor, and report on the results of information security measures of performance and mitigate all security risk?
		Is there a security and privacy awareness training policy?
		Is there a security and privacy awareness training policy?
		Does the security and privacy awareness training policy address all of the following? Purpose, Scope, Roles and Responsibilities, Management Commitment, Organizational Coordination, Compliance Measures?
		Is Basic security and privacy awareness training required as part of initial training from users?
		Is basic security and privacy awareness training provided to information system users (including managers, senior executives, and contractors)?
	Risk Assessment (ID.RA): The entity understands the cybersecurity risk to entity operations (including mission, functions, image, or reputation), entity assets, and individuals.	Does Entity have a documented vulnerability management program which is referenced in the entity's information security program plan.
		Are vulnerabilities in the information system and hosted applications scanned monthly or when changes occur to the environment and when new vulnerabilities potentially affecting the system/ applications are identified and reported?
		Does Entity has documented authenticated scan results of all assets from prior two consecutive months or more?
		Does Entity achieve a California Cybersecurity Vulnerability Metric (CCVM) score at the Moderate level or lower {< 6.9 weighted vulnerabilities per host}?
		Does Entity achieve a California Cybersecurity Vulnerability Metric (CCVM) score at the Low level (0-3.9 weighted vulnerabilities per host)?
		Are vulnerability scan reports and results from security control assessments analyzed?

NIST Cybersecurity Framework		
Function	**Category**	**Questions**
PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	Has an information system access control policy and procedures which cover all information systems within the security boundary been developed and disseminated to all employees?
		Has an information system access control policy and procedures which cover all information systems within the security boundary been developed and disseminated to all employees?
		Are there procedures in place to facilitate the implementation of access control policy?
		Does Systems implement logical password management process and enforces a minimum of 8 characters and 3 of 4 complexity types; Each password shall contain each of the following four types of characters: • English uppercase letters (A-Z) • English lowercase letters (a-z) • Westernized Arabic numerals (0-9) • Non-alphanumeric special characters (such as !,@,#,$,&,*). Does the organization employ an independent penetration agent or penetration team to perform penetration testing on the information system or system components? Does the organization employ organization-defined red team penetration tester to simulate attempts by adversaries to compromise organizational information systems in accordance with organization-defined rules of engagement? For each information system within the security boundary, has the least amount of privilege required for users to perform their job been defined? For individuals with elevated privileges (e.g., system administration), are they required to use separate accounts to access privileged and non-privileged functions? For each information system within the security boundary, are automated mechanisms employed to support the management of information system accounts, including automatically auditing account creation, modification, enabling, disabling, and removal actions? Can you provide Matrix/ spreadsheet identifying different account types, users assigned to each account type along with the Managers responsible for approving the different types of accounts?
		For each information system within the security boundary, are inactive accounts automatically disabled? What is the length of inactivity before automatically being disabled? For each information system within the security boundary, what is the frequency that users accounts are reviewed for compliance with account management requirements?

PROTECT (PR)		Is there a physical and environmental protection policy? Is the physical and environmental protection policy disseminated to Information technology personnel and executive management?
		Is there a physical and environmental protection policy? Is the physical and environmental protection policy disseminated to Information technology personnel and executive management?
		Are there procedures in place to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls?
		Are individuals from the facility access list removed when access is no longer required? Entity can demonstrate via documentation the entity's adherence to the physical security policy and procedure; this is validated by taking a relevant sample of separated employees and ensuring they no longer have active badges
		Does the physical access authorization process within the organization include verifying individual access authorizations before granting access to the facility? Are visitors escorted and visitor activity monitored according to organization-defined circumstances requiring visitor escorts and monitoring? Are keys, combinations, and other physical access devices secured? Does Entity have documented proof of semi-annual social engineering tests to test the effectiveness of the physical security policy and procedure.
		Are there information systems access control policy? For each information system within the security boundary, are users authorized remote access (i.e., through external networks such as the Internet, dial-up, etc.)
		Are there information systems access control policy for remote access? For each information system within the security boundary, are users authorized remote access (i.e., through external networks such as the Internet, dial-up, etc.)? Are there a limited number of remote access methods and access points that are authorized and monitored?
		Does the organization have documented remote access procedures for managing user identity?
		Are FIPS 140-2 cryptographic mechanisms used for remote access? Are the cryptographic mechanisms FIPS 140-2 compliant? For each information system within the security boundary, is multifactor authentication for remote access to privileged and non-privileged accounts where one of the factors is provided by a device separate from the information system?
		For each information system within the security boundary, is multifactor authentication for remote access to privileged and non-privileged accounts where one of the factors is provided by a device separate from the information system? Have Entity implemented remote access technology which identifies and alerts on anomalous remote access activity (geo-location, posture assessments, malware detection, etc?

PROTECT (PR)		Has separate sub-networks, either physically or logically, been defined for publicly accessible system components and internal organizational networks?
		For network connections, has the organization implemented a default policy to deny all network traffic and allow traffic by exception (e.g., deny all and permit by exception)?
		Are connections to networks and information systems external to the security boundary through managed interfaces of boundary protection devices (e.g., firewalls)? Has the organization limited the number of external network connections (for example, via the Trusted Internet Connection [TIC]) and can account for all such connections?
		Does the organization monitor and control communications at the external and internal boundaries of the security boundary? For network connections, have all the following parameters been implemented: a) Implemented a managed interface for each external telecommunications service b) Established network traffic flow policy for each managed interface?
		For network connections, have all the following parameters been implemented: a) Implemented protection to assure the confidentiality and integrity of information passing through each interface b) Documented exceptions to the traffic flow policy; or c) A process to review exceptions to the traffic flow policy and removes exceptions no longer necessary?
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	Is the information security and privacy awareness training policy disseminated to the appropriate stakeholders?
		Is the information security and privacy awareness training policy disseminated to the appropriate stakeholders?
		Is general and role-based security and privacy awareness training provided to personnel with assigned security roles and responsibilities?
		Are individual security and privacy awareness training records retained for one year? Does at least 80% of state entity's identified users who require role-based information security and privacy awareness training have taken the training in past 12 months? Provide evidence via relevant sample.
		Is Basic security and privacy awareness training required as part of initial training from users? Does Entity's information security and privacy awareness training occur within 30 days of personnel onboarding? Provide evidence via relevant sample.
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy	For each information system within the security boundary, has the organized identified how the confidentiality and integrity of data at rest is to be protected?
		For each information system within the security boundary, has the organized identified how the confidentiality and integrity of data at rest is to be protected? Is encryption used to protect data at rest?

PROTECT (PR)	to protect the confidentiality, integrity, and availability of information.	Have organizational requirements been implemented for the establishment and management of cryptographic keys?
		Is a manual process used for Encryption process and which requires staff to take action to enforce encryption? For each information system and application within the security boundary where cryptography is deployed, has the cryptography products been validated under the Cryptographic Module Validation Program to confirm compliance with FIPS 140-2, and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards?
		Are Mobile devices encrypted via automated method? Is FIPS 140-2 validated (enforced via MDM, GPO or 3rd party application)?
		Entity does not have a published encryption policy which covers encryption at rest for databases and non-mobile assets with confidential or sensitive data.
		Entity does not have a published encryption policy which covers encryption at rest for databases and non-mobile assets with confidential or sensitive data.
		Does the organization have documented inventory of all its data on confidential and sensitive databases and non-mobile assets?
		Does the organization encrypt its confidential and sensitive databases and non-mobile assets? For each information system and application within the security boundary where cryptography is deployed, has the cryptography products been validated under the Cryptographic Module Validation Program to confirm compliance with FIPS 140-2, and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards?
		Have organizational requirements been implemented for the establishment and management of cryptographic keys?
		Has the organized identified how the confidentiality and integrity of data in transit is to be protected?
		Has the organized identified how the confidentiality and integrity of data in transit is to be protected? Is encryption used to protect data in transit?
		For each information system and application outside the security boundary, does the organization employ cryptographic mechanisms to protect information integrity during transmission?
		For each information system within the security boundary, has the organized identified how the confidentiality and integrity of data in transit is to be protected? Is encryption used to protect data in transit? Does Entity's implemented encryption use /not any deprecated standards.
		Entity has a break and inspect point being leveraged for detection and analysis for all encrypted traffic on the network.
		Is there a current baseline configuration for the system?

PROTECT (PR)	**Information Protection Processes and Procedures (PR.IP):** Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	Is there a current baseline configuration for the system? Is the baseline configuration documented and maintained in a repository?
		Does the organization have documented configuration baselines for workstations, servers, network devices, and mobile device?
		Did the company implement configuration baselines for workstations and servers and achieve average combined assessment scores between 50% - 75% compliant, based on an approved SCAP template (e.g. USGCB or STIG as applicable) appropriate for the target Operating System?
		Entity implemented configured baselines for workstations and servers and achieved average combined assessment scores > 75% compliant, based on an approved SCAP template (e.g., USGCB or STIG as applicable) appropriate for the target Operating System?
		Entity implemented configuration baselines for workstations and servers and achieved average combined assessment scores > 75% compliant, based on an approved SCAP template (e.g., USGCB or STIG as applicable) appropriate for the target Operating System?
		Is there a configuration management policy? Is the configuration management policy disseminated to the appropriate personnel and executive management?
		Is there a configuration management policy? Is the configuration management policy disseminated to the appropriate personnel and executive management?
		Is there a change control process in place for this information system? Does the organization have a formalized change control process, including provision for emergency requests, with a security subject matter expert as a voting member?
		Does the organization perform security impact analysis prior to implementation? Are previous versions of the baseline retained for roll-back, including diagrams and organization-defined configurations? Does the organization have documented roll back process and a security impact analysis for tested changes Provide relevant evidence?
		Does the organization have an enterprise-wide single automated workflow tool for change management?
		Is there a physical and environmental protection policy? Is the physical and environmental protection policy disseminated to Information technology personnel and executive management?
		Is there a physical and environmental protection policy? Is the physical and environmental protection policy disseminated to Information technology personnel and executive management?
		Are, power, door access, temperature and humidity levels monitored at an organization-defined frequency?
		Does Entity have documented assessment of physical and environmental controls with identified gaps?

PROTECT (PR)		Is there a physical and environmental protection policy? Is the physical and environmental protection policy disseminated to Information technology personnel and executive management?
		Is there a physical and environmental protection policy? Is the physical and environmental protection policy disseminated to Information technology personnel and executive management?
		Is the physical and environmental protection policy disseminated to Information technology personnel and executive management?
		Are, power, door access, temperature and humidity levels monitored at an organization-defined frequency?
		Does Entity have documented assessment of physical and environmental controls with identified gaps?
		Is there a physical and environmental protection policy? Is the physical and environmental protection policy disseminated to Information technology personnel and executive management?
		Are, power, door access, temperature and humidity levels monitored at an organization-defined frequency?
		Does Entity have documented assessment of physical and environmental controls with identified gaps?
*** Pursuant to Government Code 6254.19, this information security record is confidential and is exempt from public disclosure.**		

NIST Cybersecurity Framework		
Function	**Category**	**Questions**
DETECT (DT)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.	Is there an audit and accountability policy?
		Does the information system audit all the following event types? User successful logins, logoffs, User failed login attempts, Data viewed, Data updated, Data deleted, Changes in data access, User accounts created, User accounts modified, User accounts deleted
		Does the organization review the audit records? Is there a documented rationale explaining why these logged events will support after-action investigations of security incidents?
		Do audit records contain the following information: Type of event? When the event occurred? Where the event occurred? The source of the event? Event outcome/end state? Individual or agent associated with the event? Does the information system provide notifications in the event of audit processing failure? Are automated mechanisms used to support all audit activities below: review? Analysis? Reporting? If yes, are their management level reviews the audit records for indications of inappropriate or unusual activity quarterly?
		Does the information system have an audit reduction and report creation capacity? Are audit records analyzed and correlated across different repositories to gain situational awareness? Are findings reported to the Security Manager and CIO?
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	Does Entity have documented network defense architecture or a network diagram depicting network security technologies in the entity?
		Does Entity have documented network defense architecture or a network diagram depicting network security technologies in the entity?
		Are the network manager and CIO notified of audit processing failure? Does the system provide e-mail notification to responsible personnel in the event of audit processing failure? Are automated mechanisms used to support all audit activities below: review? analysis? reporting? Are findings reported to the Security Manager and CIO?

DETECT (DT)		Does the organization monitor and control communications at the external and internal boundaries of the security boundary? For each information system within the security boundary, is monitoring performed to detect unauthorized local, network and remote connections? For all the information systems within the security boundary, are monitoring devices strategically placed to track specific types of transactions?
		For each information system within the security boundary, is the information system monitored to detect attacks or potential attacks?
		For each information system within the security boundary, are malicious code protection mechanisms (e.g., antivirus) deployed?
		For each information system within the security boundary, are malicious code protection mechanisms (e.g., antivirus) deployed? Do malicious code protection mechanisms scan the information system? Is real-time scanning of files received from external sources at network entry/exit points performed? In response to malicious code detection, do malicious code protection measures?
		For each information system within the security boundary, are malicious code protection mechanisms (e.g., antivirus) deployed? Does the organization manage all hosts in an enterprise anti-malware solution that provides consolidated management and reporting capabilities? Between 75% - 95% of non-stale hosts check-in and update no less than every 15 days?
		Does the organization have tools in place to detect malicious software on endpoints? Greater than 95% of expected clients under enterprise management meet all conditions within the ISA Phase II criteria?
		Are malicious code protection mechanisms automatically updated? Does the information system alert support staff if indications of compromise or potential compromise occur? For information security monitoring of all the information systems within the security boundary, are support staff and/or security personnel on email distribution or alert lists to receive security alerts, advisories, and directives? Does the organization generate and disseminate security alerts, advisories, and directives to staff and users engaged in supporting and using the information systems within the security boundary?
		Pulled from the Identify function.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and	For information security monitoring of all the information systems within the security boundary, has roles and responsibilities been developed, assigned, and documented?
		For information security monitoring of all the information systems within the security boundary, has roles and responsibilities been developed, assigned, and documented?

DETECT (DT)	adequate awareness of anomalous events.	Does Entity have documented escalation criteria within its organization with clear thresholds for communication of incidents and information needed to best inform decisions at the executive level. Are security incidents reported?
		For which of the following procedures is the IR plan reviewed, approved and followed? Distributed to IR personnel, reviewed at a defined interval, Updated to address changes needed due to implementation and testing, Initiates communication of changes to IR personnel? Does Entity has performed tabletop exercises or is able to show documentation of an incident being handled using its communication plan in the past twelve months? (NIST SI-4 (9))
		Does Entity provide relevant event metadata to Cal-CSIC and/or other relevant coordinating bodies, as appropriate?
*** Pursuant to Government Code 6254.19, this information security record is confidential and is exempt from public disclosure.**		

NIST Cybersecurity Framework		
Function	**Category**	**Questions**
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	Is there an incident response plan?
		Is there an incident response plan? Does the organization have a documented incident response plan and reports discovered incidents via Cal-CSIRS?
		Is there incident response training for users with assigned contingency roles? Does the organization train staff on incident response plans and staff understand their roles and responsibilities?
		Are incident response lessoned learned incorporated into all of the following: IR procedures IR training IR testing/exercises?
		Do Entity's users identify threat and notify cybersecurity team (in accordance with published policy) of detection of a phishing simulation in < 60 minutes of activation?
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	Is there an incident response policy?
		Is there an incident response policy?
		Are there procedures for incident response planning? Are all information system security incidents tracked and documented including non-reportable incidents?
		Are security incidents reported? Are organization's personnel required to report incidents immediately and report incidents to the CIO or other management? Do automated mechanisms support security incident reporting?
		Does the organization conduct trend analysis within the past twelve months on incidents to detect systemic issues within the organization?
*** Pursuant to Government Code 6254.19, this information security record is confidential and is exempt from public disclosure.**		

NIST Cybersecurity Framework		
Function	**Category**	**Questions**
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	
		Are lessons learned captured from annual TRP testing for any mission critical systems?
		Are lessons learned captured from annual TRP testing for at least one (1) mission critical system?
		Are lessons learned captured from annual TRP testing for all mission critical systems?
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	

*** Pursuant to Government Code 6254.19, this information security record is confidential and is exempt from public disclosure.**