FY22 California State and Local Cybersecurity Grant Program
DRAFT Maturity Assessment Survey

This survey will help identify the cybersecurity maturity of your organization and will aid in identifying how your proposed project will align with maturity and the elements denoted in the Cybersecurity Plan.

PUBLIC RECORDS ACT NOTICE

Proposals are subject to the Public Records Act, Government Code Section 7920.000, *et seq*. Do not put any personally identifiable information or private information on this proposal. If you believe that any of the information you are putting on this proposal is exempt from the Public Records Act, please indicate what portions of the proposal and the basis for the exemption. Your statement that the information is not subject to the Public Records Act will not guarantee that the information will not be disclosed.

Maturity Survey Question	Response
GOVERN	
Governance: On a scale of one to five, how clearly defined and documented are your organization's cybersecurity roles and responsibilities, including those of senior leadership? **Enter a response of 1-5 here:**	1: Roles and responsibilities are unclear or undocumented. 2: Some roles and responsibilities are defined but not consistently communicated. 3: Roles and responsibilities are documented but may not be consistently followed or reviewed. 4: Roles and responsibilities are well-documented and communicated throughout the organization. 5: Roles and responsibilities are clearly defined, communicated, and regularly reviewed for effectiveness by senior leadership.

Maturity Survey Question	Response
Risk Management: On a scale of one to five, how effectively does your organization identify, assess, and prioritize cybersecurity risks? **Enter a response of 1-5 here:**	1: Cybersecurity risks are not systematically identified or assessed. 2: There is some ad-hoc identification and assessment of risks, but it's not comprehensive or consistent. 3: Risks are identified and assessed periodically, but prioritization may not be aligned with organizational objectives. 4: Risks are systematically identified, assessed, and prioritized based on business impact and likelihood. 5: There is a mature risk management process in place that continuously monitors and adapts to evolving threats and vulnerabilities.
Compliance: On a scale of one to five, how well does your organization ensure compliance with relevant cybersecurity standards, regulations, and contractual obligations? **Enter a response of 1-5 here:**	1: Compliance efforts are ad-hoc or reactive, with little formalized processes in place. 2: Compliance is considered, but efforts are not consistently tracked or monitored. 3: Compliance with regulations and standards is generally maintained, but gaps may exist in documentation or implementation. 4: There are formal processes for tracking and documenting compliance with relevant standards and regulations. 5: Compliance is actively managed, with regular audits, assessments, and continuous improvement initiatives in place.

Maturity Survey Question	Response
IDENTIFY	
Asset Management: On a scale of one to five, how effectively does your organization identify and manage its assets (e.g., devices, systems, data)? **Enter a response of 1-5 here:**	1: There is little to no formalized process for asset inventory and management. 2: Asset management is partially implemented, but there are gaps in visibility or accuracy. 3: Assets are generally identified and tracked, but the process may not be fully automated or integrated. 4: There is a comprehensive asset management program in place, with automated tools and processes for continuous discovery and monitoring. 5: Asset management is highly mature, with real-time visibility into all assets and their associated risks.
Risk Assessment: On a scale of one to five, how robust is your organization's approach to risk assessment? **Enter a response of 1-5 here:**	1: Risk assessment is not conducted or is sporadic and informal. 2: There are ad-hoc risk assessments, but they are not standardized or comprehensive. 3: Risk assessments are conducted periodically, but there may be gaps in coverage or depth. 4: There is a formalized risk assessment process that covers all critical assets and threats, with documented methodologies and criteria. 5: Risk assessments are integrated into business processes, conducted continuously, and dynamically adjusted based on emerging threats and changes in the environment.

Maturity Survey Question	Response
Threat Intelligence Integration: On a scale of one to five, how effectively does your organization integrate external threat intelligence into its cybersecurity strategy? **Enter a response of 1-5 here:**	1: There is minimal awareness or integration of external threat intelligence. 2: Some basic threat intelligence sources are utilized, but integration is ad-hoc. 3: Threat intelligence feeds are monitored periodically, but there is limited integration into security operations. 4: Threat intelligence is actively collected, analyzed, and integrated into security processes and decision-making. 5: There is a mature threat intelligence program in place, with automated feeds, advanced analytics, and proactive response mechanisms based on intelligence insights.
PROTECT	
Access Control: On a scale of one to five, how robust are your organization's access control measures to protect sensitive information and critical systems? **Enter a response of 1-5 here:**	1: Access controls are minimal or non-existent, with little restriction on user privileges. 2: Basic access controls are in place, but they may not be consistently enforced or monitored. 3: Access controls are implemented for most systems and data, with periodic reviews of user access rights. 4: Access controls are well-defined, consistently enforced, and integrated with identity management systems. 5: Access controls are highly mature, leveraging advanced techniques such as multi-factor authentication, least privilege access, and continuous monitoring.

Maturity Survey Question	Response
Data Security: On a scale of one to five, how effectively does your organization protect sensitive data from unauthorized access or disclosure? **Enter a response of 1-5 here:**	1: Data protection measures are minimal, with little encryption or data classification. 2: Some data protection measures are in place, but they may not cover all sensitive data or be consistently applied. 3: Data protection measures are implemented for sensitive data, with encryption and access controls based on data classification. 4: Data protection practices are well-defined and integrated into business processes, with regular audits and compliance checks. 5: Data protection measures are highly mature, with robust encryption, data loss prevention (DLP) controls, and comprehensive data lifecycle management.
Security Awareness and Training: On a scale of one to five, how effective are your organization's efforts to promote cybersecurity awareness and provide training to employees? **Enter a response of 1-5 here:**	1: There is minimal cybersecurity awareness or training provided to employees. 2: Basic cybersecurity training is conducted sporadically, with limited coverage of key topics. 3: Regular cybersecurity training is provided to employees, covering essential topics such as phishing awareness and password security. 4: Security awareness programs are well-established, with tailored training modules and ongoing reinforcement activities. 5: Security awareness and training programs are highly mature, incorporating advanced techniques such as simulated phishing exercises, role-based training, and gamification.

Maturity Survey Question	Response
DETECT	
Incident Detection Capability: On a scale of one to five, how capable is your organization in detecting cybersecurity incidents in a timely manner? **Enter a response of 1-5 here:**	1: Incident detection capabilities are minimal, relying mainly on manual monitoring and reactive responses. 2: Some basic detection mechanisms are in place, but they may not cover all potential threats or be consistently monitored. 3: Incident detection tools and processes are implemented for key assets and systems, with periodic reviews and improvements. 4: Advanced detection technologies such as intrusion detection systems (IDS), security information and event management (SIEM), and endpoint detection and response (EDR) are deployed and actively monitored. 5: Incident detection capabilities are highly mature, with continuous monitoring, automated response mechanisms, and integration with threat intelligence feeds.
Log Management and Analysis: On a scale of one to five, how effectively does your organization collect, analyze, and correlate security logs to identify potential security incidents? **Enter a response of 1-5 here:**	1: Logging and analysis capabilities are minimal, with limited collection and retention of security logs. 2: Some basic log management tools are in place, but they may not capture all relevant security events or provide meaningful analysis. 3: Log management and analysis tools are deployed for critical systems, with regular reviews of logs and alerts. 4: Centralized logging infrastructure and advanced analytics tools are used to correlate security events across the organization, enabling proactive detection and response. 5: Log management and analysis capabilities are highly mature, with real-time monitoring, correlation of disparate data sources, and automated incident response workflows.

Maturity Survey Question	Response
Anomaly Detection and Behavioral Analysis: On a scale of one to five, how mature are your organization's capabilities in detecting anomalous behavior and suspicious activities on the network and endpoints? **Enter a response of 1-5 here:**	1: Anomaly detection capabilities are minimal, with no dedicated tools or processes for identifying abnormal behavior. 2: Some basic anomaly detection techniques are employed, but they may not effectively differentiate between normal and malicious activities. 3: Anomaly detection tools are deployed and configured to monitor network and endpoint behavior, with regular tuning and refinement. 4: Advanced behavioral analysis techniques such as machine learning and user behavior analytics (UBA) are integrated into the detection process, enabling early detection of sophisticated threats. 5: Anomaly detection and behavioral analysis capabilities are highly mature, with continuous monitoring, baselining of normal behavior, and adaptive response to emerging threats.
RESPOND	
Incident Response Planning: On a scale of one to five, how comprehensive and well-documented is your organization's incident response plan? **Enter a response of 1-5 here:**	1: There is no formal incident response plan in place. 2: An incident response plan exists, but it's outdated, incomplete, or not widely known throughout the organization. 3: The incident response plan is documented and regularly reviewed, with defined roles, responsibilities, and procedures. 4: The incident response plan is periodically tested through tabletop exercises or simulations, and updates are made based on lessons learned. 5: The incident response plan is highly mature, regularly tested through realistic scenarios, integrated with business continuity planning, and continuously improved based on feedback and changes in the threat landscape.

Maturity Survey Question	Response
Incident Response Team Capability: On a scale of one to five, how capable and prepared is your organization's incident response team to handle cybersecurity incidents? **Enter a response of 1-5 here:**	1: There is no dedicated incident response team or formalized process for incident handling. 2: Some individuals within the organization are designated to respond to incidents, but their training and capabilities may be limited. 3: A dedicated incident response team exists, with defined roles and responsibilities, and members receive periodic training and skill development. 4: The incident response team is well-trained and experienced in handling various types of incidents, with documented procedures for escalation and coordination. 5: The incident response team is highly skilled, with specialized expertise in different areas of cybersecurity, and is capable of responding swiftly and effectively to complex and coordinated cyberattacks.
Communication and Coordination: On a scale of one to five, how effective is your organization's communication and coordination during incident response efforts? **Enter a response of 1-5 here:**	1: Communication and coordination during incidents are ad-hoc or chaotic, leading to delays or misunderstandings. 2: There are basic communication channels in place, but they may not be well-defined or consistently utilized during incidents. 3: Communication protocols are established, and incident response teams are trained in effective communication and coordination practices. 4: During incidents, communication channels are promptly activated, stakeholders are informed, and coordination among teams is facilitated through established procedures. 5: Communication and coordination during incident response are highly mature, with real-time collaboration tools, predefined communication channels, and clear escalation paths for different scenarios.

Maturity Survey Question	Response
RECOVER	
Backup and Recovery Capability: On a scale of one to five, how robust and comprehensive is your organization's backup and recovery capability for critical systems and data? **Enter a response of 1-5 here:**	1: There is no formalized backup and recovery strategy in place. 2: Basic backup procedures are implemented, but they may not cover all critical systems or data, and recovery processes are not regularly tested. 3: Backup and recovery processes are documented, with regular backups taken and tested for critical systems and data, but there may be some gaps or inconsistencies. 4: Automated backup solutions are deployed, with regular backups, offsite storage, and documented recovery procedures that are periodically tested and updated. 5: Backup and recovery capabilities are highly mature, with continuous data protection, real-time replication, automated failover, and rigorous testing of recovery plans to ensure rapid restoration of services.
Incident Recovery Planning: On a scale of one to five, how well-prepared is your organization to recover from cybersecurity incidents and disruptions to business operations? **Enter a response of 1-5 here:**	1: There is no formal incident recovery plan in place. 2: An incident recovery plan exists, but it's outdated, incomplete, or not widely known throughout the organization. 3: The incident recovery plan is documented and regularly reviewed, with defined roles, responsibilities, and procedures for restoring critical systems and services. 4: The incident recovery plan is periodically tested through tabletop exercises or simulations, and updates are made based on lessons learned from past incidents. 5: The incident recovery plan is highly mature, regularly tested through realistic scenarios, integrated with business continuity planning, and continuously improved based on feedback and changes in the threat landscape.

Maturity Survey Question	Response
Resilience and Continuity Measures: On a scale of one to five, how resilient are your organization's systems and processes to withstand and recover from disruptive events? **Enter a response of 1-5 here:**	1: There are no formal resilience or continuity measures in place. 2: Basic resilience measures are implemented, but they may not cover all critical systems or processes, and there is limited redundancy or failover capability. 3: Resilience measures are documented and implemented for critical systems and processes, with redundancy, failover, and recovery plans in place, although some gaps may exist. 4: Resilience measures are actively monitored and maintained, with automated failover and recovery mechanisms for critical systems, and regular testing of continuity plans. 5: Resilience measures are highly mature, with advanced redundancy, fault tolerance, and self-healing capabilities integrated into the infrastructure, and continuous monitoring and optimization to adapt to evolving threats and requirements.