Bay Area Regional Cyber Incident Response Framework

Version 1.0

September 2020

This page intentionally left blank

RECORD OF CHANGES

This Bay Area Regional Cyber Incident Response Framework should be reviewed annually to identify areas that may require updates or additions as the Bay Area Urban Areas Security Initiative (UASI) and its jurisdictions and partners continue to build and mature their cybersecurity programs, capabilities, and services. As necessary, based on the annual review, the Framework should be updated to ensure it reflects current cybersecurity priorities and concepts. Table 1 should be updated to reflect revisions.

Table 1: Record of Changes

Change Number	Section	Date of Change	Individual Making Change	Description of Change

This page intentionally left blank

TABLE OF CONTENTS

This page intentionally left blank

EXECUTIVE SUMMARY

The Bay Area UASI, in conjunction with the Northern California Regional Intelligence Center (NCRIC), is pleased to share the Bay Area Regional Cyber Incident Response Framework. The purpose of the Framework is to assist Bay Area organizations to strengthen their cyber incident response capabilities as well as region-wide coordination in managing the impacts of cyber incidents. The Framework aims to enhance capabilities, efforts, and capacity across individual organizations, operational areas, and the region as shown in **Figure 1**—it's critical to tackle all three to enhance resilience. The Framework is designed to cover cyber planning and response information in a user-friendly format to encourage active engagement.

Figure 1: Regional Cyber Incident Response Framework Focus Areas

The Framework is the culmination of the current Bay Area UASI Cybersecurity Incident Response Framework Planning Project beginning in June 2019. Throughout the project, the Bay Area UASI and NCRIC have engaged in region-wide cyber planning efforts, working closely with the Cyber Resilience Work Group. We developed and conducted a region-wide cybersecurity preparedness survey and cyber plan review, establishing a baseline understanding of the region's cyber capabilities and capacity.

These efforts informed the 2020 Bay Area UASI Cybersecurity Preparedness Workshop, where stakeholders in information technology (IT), information security, and emergency management roles across government, regional, non-profit, and private sector entities discussed their cyber planning needs. We collected cyber priorities intimated by Bay Area representatives as well as lessons learned throughout this project to develop a cyber planning toolkit. The cyber toolkit, including cyber planning templates, were debuted in a July workshop and are now available on the Bay Area UASI's Cybersecurity webpage. Following the workshop, our team turned our attention to the final task, developing and delivering the Regional Cyber Incident Response Framework.

The Bay Area UASI and NCRIC are proud to offer this Framework to help communities prepare for, respond to, and recover from cyber incidents. We look forward to continued collaboration across the region to build and strengthen our cyber resilience.

Sincerely,

Mikyung Kim-Molina,
Bay Area UASI Regional Project Manager

Alison Yakabe,
NCRIC Cyber Security Team Lead Analyst

Framework Overview

The Framework is designed to review organizational/local, county-wide/operational area, and region-wide cyber information and is organized as follows:

- ***Executive Summary*** provides background information on the Framework and the wider Bay Area Cybersecurity Incident Response Framework Planning Project.
- ***Organizational/Local Cyber Incident Response*** outlines information and resources to assist organizations in determining and building their cyber preparedness.
- ***County-wide/Operational Area Cyber Incident Response*** discusses formal and informal relationship building and resource sharing, in addition to outlining mutual aid and defining Cyber Incident Response Teams.
- ***Region-wide Cyber Incident Response*** provides a brief summary of key features of region-wide coordination.
- ***Appendix A: NIST Framework Guidance*** explains how organizations and jurisdictions can use the NIST Framework to identify opportunities to strengthen their risk management and cybersecurity programs as well as to communicate their programs to partners.
- ***Appendix B: Bay Area Cyber Preparedness Survey Methodology and Analysis*** provides additional details on the survey analysis methodology and results.
- ***Appendix C: Bay Area Cybersecurity Training Options*** includes recommendations on region-wide cyber training priorities and available resources.
- ***Appendix D: Mutual Aid Agreement Considerations*** offers guidance to reference when drafting a mutual aid agreement.
- ***Appendix E: Glossary and Acronyms*** references all terms and acronyms provided in the Framework.

ORGANIZATIONAL/LOCAL CYBER INCIDENT RESPONSE

Bay Area Region-wide Cyber Preparedness

In late 2019, the Bay Area UASI engaged representatives from the 12 counties and three core cities in the Bay Area to develop and deliver the Cyber Preparedness Survey. The survey addressed six key focus areas, including planning, incident response, resources, training and exercises, and threat landscape. Survey participants included Chief Information Officers (CIO), Chief Information Security Officers (CISO), and emergency managers across government, non-governmental organizations (NGO), and the private sector. Through this survey and subsequent tasks, a baseline understanding was developed of the Bay Area UASI's cybersecurity preparedness and response capabilities. More information on the methodology and analysis of these findings are provided in **Appendix B: Bay Area Cyber Preparedness Survey Methodology and Analysis.**

The goal was to determine useful tools and resources for organizations and jurisdictions to develop an enhanced approach to cybersecurity, and identify specific strengths, gaps, and opportunities to inform future cyber project tasks.

In reviewing Bay Area survey results and general cybersecurity best practices, several critical elements rose to the top, as highlighted in **Figure 2.** Organizations were more confident in their cyber incident response capacity when they had:

- A dedicated cybersecurity professional within senior leadership;
- An organizational cyber plan;
- A process for mutual aid; and
- A higher budget for cybersecurity.

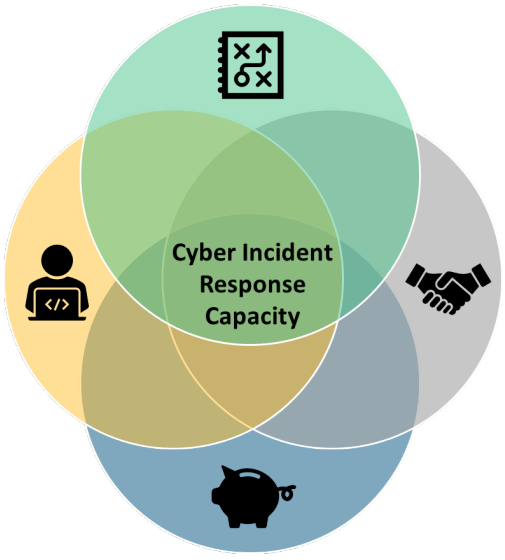

Figure 2: Several elements impacted organizational confidence in their cyber incident response capacity within our survey results

When these elements are not in place, organizations tended to rate themselves as less capable in cyber incident response. The key to building capabilities is to understand the organization's current cyber planning posture, including strengths and areas for improvement. When addressing any gaps in cyber preparedness, organizations may consider addressing some of the items covered above. In particular, organizations may consider broadening from mutual aid considerations to wider surge capabilities and processes for external assistance. Much of this Framework offers guidance on how to form and maintain relationships, engage in cyber planning to identify needed resources or external assistance (such as cyber insurance), and conduct cyber incident response operations effectively region-wide.

Engage in Cyber Planning

Bay Area UASI Cyber Toolkit

The Bay Area UASI region developed a Cyber Toolkit to assist organizations/jurisdictions with cyber planning, including several resources that can be used to increase cyber incident preparedness and response effectiveness. The Cyber Toolkit includes the **Technology Recovery Plan (TRP) template**, and the **Cyber Incident Response Plan (CIRP) template**. Your organization/jurisdiction can use these templates to facilitate cyber planning, working with parties to customize with specific information relevant to your entity. These templates are designed to help you develop your own cyber plans that enable your organization/jurisdiction to quickly identify, respond to, and recover from cyber incidents.

The TRP serves as the guide to quickly redirect available resources towards IT systems recovery and restoration The TRP enables the efficient recovery of critical systems and helps your jurisdiction/organization avoid further damage or disruption to critical business functions. Executing this plan will minimize recovery time and possible delays, improve security, and mitigate potentially damaging impacts caused by taking action without a clearly defined and tested plan.

Using the TRP template, your organization/jurisdiction can identify recovery priorities and procedures and a communication plan for cyber incident response.

The CIRP is vital to ensuring that an organization/jurisdiction responds quickly and effectively to a cyber incident. A CIRP provides the direction required to effectively assess and respond to any type of cyber incident and its cascading effects. These incidents may include malware, ransomware, or a distributed denial of service (DDoS) attack, among many others. When a cyber incident occurs, it is critical to have a plan in place that describes the specific actions and procedures the organization/jurisdiction should perform (e.g., notification and escalation decision points, analysis and identification processes, containment actions). This will help minimize damage, reduce disaster response times, and mitigate breach-related expenses.

The CIRP template provides the guidance needed to develop an actionable cyber incident response plan, including a clear strategy for information sharing.

Additionally, there is a direct relationship between cyber and Continuity of Operations (COOP) planning. COOP planning includes the business process analysis (BPA), business impact analysis (BIA), and the COOP Plan as highlighted below:

- Through a **BPA**, an organization identifies the functional processes, activities, personnel expertise, systems, data, interdependencies, alternate locations, and other Essential Assets (EAs) needed to perform Essential Functions (EFs).
- An organization uses a **BIA** to identify and prioritize those EAs/EFs and determine impacts if they are disrupted. The BPA/BIA data allows for the application of organization-wide risk analysis to contribute to sound decision-making and strengthens operations through effective risk management.
- The **COOP Plan** builds on the BIA, including a narrative on how an organization will restore its EFs at an alternate site and perform them until they are able to return to normal operations.
- For more information on COOP and associated tools and templates, please see the Bay Area UASI's COOP/Continuity of Government (COG) Toolkit.

Nationwide Cybersecurity Review

The Nationwide Cybersecurity Review (NCSR) is a no-cost, anonymous, annual self-assessment that is designed to measure gaps and capabilities of state, local, tribal and territorial (SLTT) governments' cyber programs. The NCSR is aligned to the NIST Cybersecurity Framework and is sponsored by the Department of Homeland Security (DHS) and the MS-ISAC.

Under the 2019 UASI grant, there were a total of 19 Bay Area jurisdictions that completed the NCSR as part of the Bay Area UASI's cyber project.

Participating in the NCSR may raise cyber awareness and communication within your organization and with critical stakeholders. By participating, your organization creates a cybersecurity baseline which can be used to develop your future security roadmap. You may also track progress over time, comparing your scores against previous scores as well as against the aggregate scores of your peers across the nation. Submitting your organization's NCSR may also make you eligible for grant funding. NCSR users can also access cybersecurity tools, including reports and templates. Learn more at https://www.cisecurity.org/ms-isac/services/ncsr/.

Assessing Cyber Preparedness Using the NIST Framework

As demonstrated by the survey results above, many jurisdictions in the Bay Area would be more confident in their cybersecurity posture if they engage in targeted cyber planning. To that end, the National Institute of Standards and Technology (NIST) Framework supports a risk-based approach to developing or improving a cyber program. The Framework is voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders.

The NIST Framework integrates industry standards and best practices to help organizations effectively manage their cybersecurity risks.

The NIST Framework is a tool that jurisdictions can use within their existing cybersecurity programs to identify opportunities to strengthen their risk management and cybersecurity programs as well as to communicate their programs to partners. For those that do not already have a cybersecurity program, organizations can use the NIST Framework to develop one.

The NIST Framework is a flexible tool that supports organizations to develop the appropriate level of cybersecurity through "implementation tiers" that suit the needs of each organization. The implementation tiers are designed to identify a path for organizations to incorporate cyber risk into the overall organizational risk. Reaching the highest tier of capability requires a substantial level of resources (e.g., funding, staff, equipment, systems, policies, procedures, training). It is not realistic for every jurisdiction in the Bay Area to achieve the same tier. Each jurisdiction designs its own program to achieve the appropriate tier, based on a risk-informed approach, through a deliberate process.

To use the NIST Framework to develop or improve their cybersecurity program, jurisdictions must:

1. Describe their current cybersecurity posture;
2. Describe their target state for cybersecurity;
3. Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
4. Assess progress toward the target state; and

5. Communicate among internal and external stakeholders about cybersecurity risk.

For details on the NIST Framework and how jurisdictions can use it to inform and improve their cybersecurity programs, refer to **Appendix A: NIST Framework Guidance**.

Determine Cyber Needs

No organization possesses all of the capabilities required to be fully prepared for a cyber incident. External partners can offer critical resources, services, information, and perspective that may help prevent a cyber incident, mitigate the impacts of an incident, and help ensure a quick, effective incident recovery. Organizations should seek to augment their capabilities and enhance understanding of the current cyber threat environment. This should include identifying what partners and external services you currently rely on and how additional partners, services, and resources may enhance your cyber program.

Follow a Simple Roadmap after a Cyber Incident

After a suspected or actual cyber incident, your organization should activate its existing cyber plans (e.g., CIRP and TRP). If your organization does not have cyber plans, refer to the Bay Area Cyber Toolkit for templates that will enable you to develop your own CIRP and TRP. At a high level, there is a simple roadmap that your organization should follow in the absence of a cyber plan (or as part of a developed plan). This roadmap, depicted in **Figure 3**, can help ensure that, at a minimum, your organization notifies the appropriate parties to get the guidance and direction that can be critical during incident response. Note that some organizations opt into purchasing cyber insurance to help them mitigate loss and damages as a result of cyber incidents—more information on cyber insurance may be found in the **External Cyber Incident Response Resources** section. For those organizations that do not have cyber insurance, skip Step 2 and move directly to contacting the NCRIC.

Figure 3: Roadmap for Coordination Following a Cyber Incident

NCRIC Cyber Capabilities and Offerings

The NCRIC is the Bay Area's nationally renowned "All Crimes Fusion Center" staffed, operated, and managed by representatives from local public safety agencies in the region with oversight from the Northern California High Intensity Drug Trafficking Area (NCHIDTA) Executive Board. The NCRIC provides regional analytical and investigative support to local, state and federal law enforcement agencies involving terrorism, cybersecurity, information sharing, risk management and infrastructure protection.

The NCRIC is part of the National Network of Fusion Centers, as highlighted in **Figure 4**. The NCRIC Cybersecurity Team's mission is to deliver strategic threat intelligence, facilitate collaboration among regional cybersecurity personnel and communities of interest, and conduct network vulnerability assessment engagements, to identify and mitigate cybersecurity risk throughout the region.

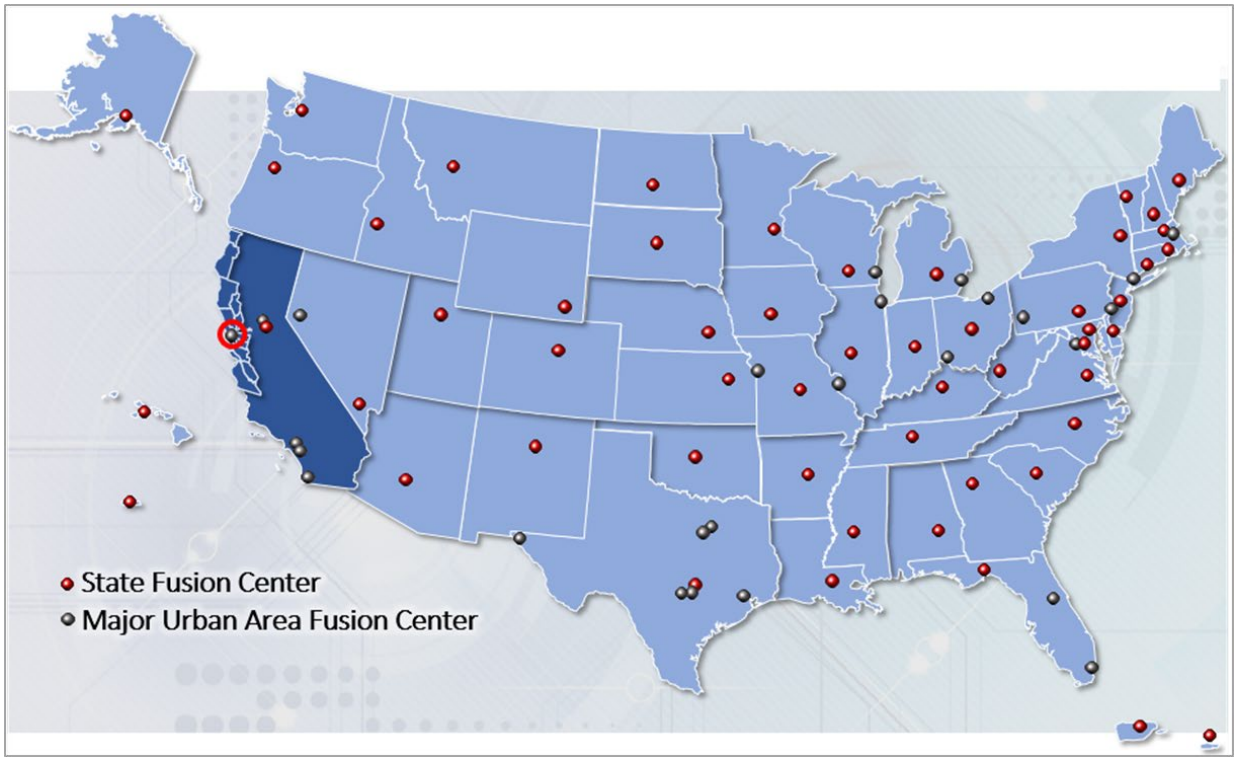

Figure 4: The NCRIC is a Major Urban Fusion Center, leading the region in cybersecurity resilience

The NCRIC Cybersecurity Team offers services such as assessments for vulnerability to known or published exploits, email phishing exercises, and phishing email analysis. Cybersecurity suspicious activity reports are collected and analyzed, to track regional trends and support awareness and preparedness. In all situations, the team adheres strictly to a policy of protecting victim identities. Finally, the NCRIC provides curated or targeted threat briefings to specific audiences or sectors; previous examples include senior leadership in healthcare or technology staff in law enforcement.

State of California Cyber Incident Response Guidance

The California Governor's Office of Emergency Services (Cal OES), through the California Cybersecurity Integration Center (Cal-CSIC), is assigned to lead California's Cybersecurity Emergency Support Function 18 (CA-ESF 18) based on its authorities, resources, and capabilities. The purpose and mission of CA-ESF 18 is to coordinate for cyber critical response including the detection, mitigation, and information sharing related to statewide cyber-related events.

Cal OES advises that non-state organizations, including local, tribal, and territorial entities, should coordinate with their Regional Fusion Centers (RFCs) during cyber incident response. RFCs provide intelligence and response capabilities which can contribute to the mission of CA-ESF 18. In the Bay Area, the RFC is the NCRIC.

Figure 5 shows the desired communications flow between CA-ESF 18 Coordination Team entities, including when a cyber incident originates within a local, tribal, or territorial entity. As detailed in Figure 3 above, the affected organization should alert their CISO in accordance with their cyber plan(s) and contact their cyber insurance provider prior to reaching out to the NCRIC. The NCRIC would then work with the organization by connecting them with the right resources, including local, state (including the State Threat Assessment Center [STAC]), and federal partners. The NCRIC provides regional situational awareness to alert jurisdictions to recent or ongoing cyber incident, redacting any personally identifiable information on the affected entities.

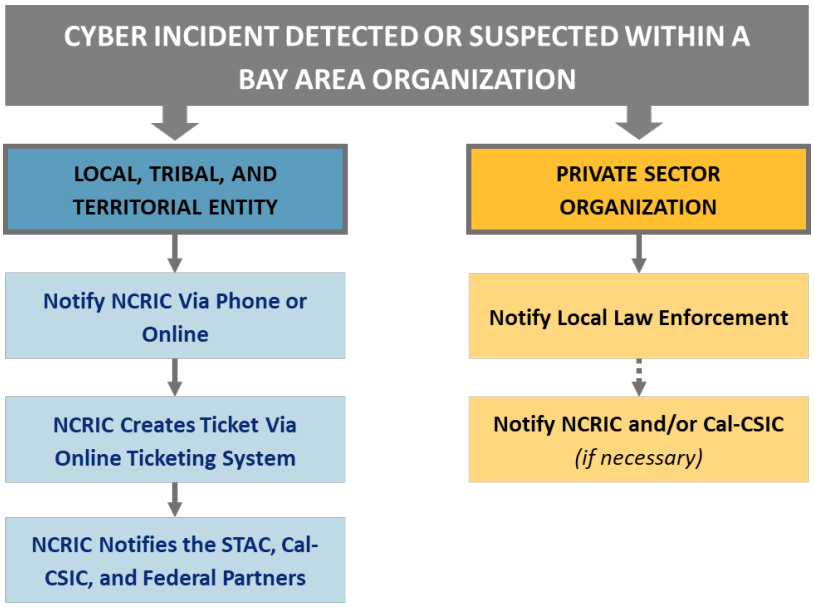

Figure 5: Cyber Incident Response Lines of Coordination

Additional Partners

In addition to the NCRIC, Bay Area organizations have access to a variety of partners who can provide support before, during, and after a cyber incident including those listed in Table 2 below. It is critical that organizations forge relationships before an incident so that you can quickly call upon your partners and they understand your cybersecurity capabilities, gaps, and other key aspects of your cybersecurity posture. These steady-state relationships help to build trust between partners, which is vital when a cyber incident requires close coordination and collaboration.

Organizations should reach out to their partners regularly to maintain relationships and ensure they are up to date on available services. Being proactive can save precious time during incident response.

Table 2: Additional Partners Available to Bay Area Entities

Potential Partner	Description of Services	Contact Information
DHS / Cybersecurity and Infrastructure Security Agency (CISA)	CISA works with public and private sector partners to share information, build greater trust, and lead the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure. CISA provides cyber assessments through National Cybersecurity Assessments and Technical Services (NCATS)—currently, participants have access to a range of cybersecurity assessments provided through CISA, including cyber resilience review, external dependencies management, cyber infrastructure survey, and vulnerability scanning. CISA is also involved in asset response, namely through the CISA Integrated Operations Coordination Center (CIOCC), formerly known as the National Cybersecurity & Communications Integration Center (NCCIC).	▪ For more information on the NCATS, visit https://www.cisa.gov/critical-infrastructure-vulnerability-assessments and/or email ncats_info@hq.dhs.gov. ▪ To report suspected or confirmed cyber incidents and seek assistance in removing the adversary, restoring operations, and recommending ways to further improve security, contact the CIOCC at ciocc.cyber@hq.dhs.gov or 888-282-0870.
Federal Bureau of Investigation (FBI)	The FBI has Cyber Task Forces (CTFs) in all 56 field offices to focus exclusively on cybersecurity threats. In addition to key law enforcement and homeland security agencies at the state and local level, each CTF partners with many of the federal agencies that participate in the National Cyber Investigative Joint Task Force at the headquarters level. This promotes effective collaboration and deconfliction of efforts at both the local and national level. The CTF role within the field office territory includes: 1) responding to cyber incidents and conducting victim-based investigations; 2) understanding and addressing the threats, vulnerabilities, and collection opportunities that exist; and 3) maintaining relationships and information sharing with key companies and institutions.	▪ Contact the Regional Cyber Task Force (Sacramento) at 857-386-2000.
United States Secret Service (Secret Service)	In March 2020, in recognition of the growing convergence of cyber and traditional financial crimes, the Secret Service began the process of merging its Electronic Crimes Task Forces and Financial Crimes Task Forces into a single unified network, what is now known as the Cyber Fraud Task Force (CFTF). The Secret Service has operationalized CFTFs in 42 domestic offices and in two international locations, London and Rome. In the coming years, the Secret Service plans to further extend the network CFTFs through it's over 160 offices across the country and around the globe.	▪ Contact the Secret Service at gioc@usss.dhs.gov or 415-576-1210

Potential Partner	Description of Services	Contact Information
Cal-CSIC	Cal-CSIC's responsibilities are broad and include: developing a statewide cybersecurity strategy; overseeing a Cyber Incident Response Team, which serves as California's primary unit in cyber threat detection, reporting, and response for the public and private sectors; assisting law enforcement partners in criminal investigations of cyber-related incidents; collecting and sharing cyber threat information among state agencies, utilities, academic institutions, private companies, and others throughout the state; providing warnings of cyberattacks to government agencies and nongovernmental partners; supporting public and private sector partners in protecting their vulnerable infrastructure and IT networks; and assessing risks to critical infrastructure and IT networks.	▪ Go to Cal-CSIC's website at https://calcsic.org/ to register for an account to receive threat intelligence and advisories from Cal-CSIC. ▪ Contact Cal-CSIC at 916-636-2997. ▪ Organizations can forward phishing emails to the Cal-CSIC at calcsic@caloes.gov so that other statewide jurisdictions and organizations can benefit from this information.
The California Governor's Cybersecurity Task Force	The California Cybersecurity Task Force is a statewide partnership comprised of key stakeholders, subject matter experts, and cybersecurity professionals from California's public sector, private industry, academia, and law enforcement. The Task Force serves as an advisory body to the State of California Senior Administration Officials in matters related to Cybersecurity. By fostering a culture of cybersecurity through education, information sharing, workforce development and economic growth, the Task Force hopes to advance the State's cybersecurity and position California as a national leader and preferred location for cyber business, education, and research.	▪ Contact the Cybersecurity Task Force at 916-636-2959 and mario.garcia@caloes.ca.gov.
MS-ISAC	The mission of the MS-ISAC is to improve the overall cybersecurity posture of the nation's SLTT governments through focused cyber threat prevention, protection, response, and recovery. MS-ISAC provides services such as advisory calls, emergency triage, remediation guidance, recovery assistance, log analysis, and forensics.	▪ The MS-ISAC Security Operations Center is available 24/7 at 866-787-4722 and soc@msisac.org. ▪ Membership in the MS-ISAC is open to employees or representatives from all 50 states, the District of Columbia, U.S. Territories, local and tribal governments, public K-12 education entities, public institutions of higher education, authorities, and any other non-federal public entity in the US. To join the MS-ISAC, go to https://learn.cisecurity.org/ms-isac-registration. ▪ For non-governmental entities, subscribe to MS-ISAC cybersecurity webinars, newsletters, and advisories on known vulnerabilities in popular software at https://learn.cisecurity.org/ms-isac-subscription.

COUNTY-WIDE/OPERATIONAL AREA CYBER INCIDENT RESPONSE

Develop Relationships to Support Cyber Planning

This section will highlight several best practices for how to develop, maintain, and strengthen relationships within your county. This will facilitate a community immersed in cyber preparedness in a "left of boom" environment, encouraging information sharing and creating informal mechanisms for helping each other. It is critical to note that support may take a variety of forms, with many opportunities for virtual support. This could include reaching out to partners for guidance or to share ideas related to cybersecurity.

Within a county, cybersecurity programs, capabilities, and available resources can vary widely. Moreover, as organizations operate within varying threat environments, some have more experience in cyber preparedness, response, and recovery efforts than others. For these reasons, it is strongly recommended that you establish relationships within your county ahead of an incident. Cultivating these relationships enables you to share information and best practices, build a shared infrastructure (e.g., determine the best communication methods and platforms to engage in information sharing), and assess partner capabilities and gaps against your own to enhance your cyber posture. This also paves the road for more formal agreements, including mutual aid.

Based on your organizational assessment, you should have a foundation for the capabilities you offer and/or gap areas where you could use assistance from a trusted partner.

Once relationships have been established, it is important to maintain and strengthen them over time. This can be done through regular meetings—virtual or in person. Informal virtual approaches to coordination outside of traditional meetings can work well too. For example, establishing Microsoft Teams or Slack groups with your counterparts across the county can facilitate rapid information sharing and can allow you to discuss cybersecurity issues, questions, or other topics.

County Cyber Planning and Response Resources

Many local entities do not have a cybersecurity program or have a very limited program, which makes it almost impossible to implement an effective security posture. Moreover, even in cases where they seek support from an external service, they may not have the required funding or cyber vendors may not be interested in providing support for very small local entities.

Counties can help address this problem by extending county services to local entities through informal agreements as well as formal mutual aid agreements. For example, a county may have an email security system in place that is working well for them. To add a small local entity to be protected under that system (e.g., a water district or a library), the county may work with them to add them under the agreement the county already has with the vendor. This is much less effort for the county to do—as opposed to having the local entity attempt to procure the service—as the county already has the processes in place and the people required to support it. Having some form of resource sharing initiated at the county level that offers those types of services at cost would allow the county to strengthen the whole community without unduly burdening the county. This simple action performed during steady state may help mitigate cyber incidents, reducing the potential need for county assistance during cyber incident response.

Establish Cyber Incident Response Teams

A Cyber Incident Response Team (CIRT) is a concrete organizational entity (i.e., one or more staff) that is assigned responsibility for coordinating and supporting the response to a cyberattack.[1] A CIRT should assess, document, and respond to a cyber incident so that a network can both recover quickly and mitigate future incidents. The CIRT's success depends on the relationships both across the organization and with trusted partners, preferably established during steady state.

Local Government staff can be identified to serve on City, County or Operational Area CIRT. A CIRT can be deployed intra-county via SEMS and the Operational Area mechanism. Region-wide CIRT deployment can be considered depending on the scale and complexity of an incident. In such cases, California Mutual Aid protocols are referenced in the **Region-wide Cyber Incident Response** section and **Appendix D: Mutual Aid Agreement Considerations** and can be referred to for guidance.

[1] Definition adapted from Robin Ruefle, Carnegie Mellon University, *Defining Computer Security Incident Response Teams*, https://us-cert.cisa.gov/bsi/articles/best-practices/incident-management/defining-computer-security-incident-response-teams, January 24, 2007

REGION-WIDE CYBER INCIDENT RESPONSE

The Bay Area contains a wide variety of jurisdictions with unique cybersecurity needs, capabilities, resources, and experience in cyber incident response. While all jurisdictions face an increasing and evolving cyber threat, each Bay Area jurisdiction has a different cyber risk profile. On their own, jurisdictions may lack a critical component in their cyber program that makes a cyber incident more likely or makes it more challenging to respond to and recover from an incident. **As a region, jurisdictions can coordinate strategically to enhance the cybersecurity posture of the entire Bay Area.**

Form and Maintain Relationships

During an actual or suspected cyber incident, a timely response is critical and even a short delay spent seeking out information on available resources can result in serious impacts to your organization. For this reason, it is important to establish relationships—both within your county and region-wide—ahead of an incident. In addition to relationships built with counterparts in your county, refer to the **Additional Partners** section above for more information on other potential regional, federal, and NGO partners.

It is highly recommended that you establish, maintain, and foster these relationships to build trust and understanding. This can be done through formal or informal approaches, both in-person and virtually, to facilitate real-time information sharing and discussion of cybersecurity issues and questions.

Develop a Shared Understanding of Cyber Incident Response Support

External partners can make the difference between a minor cyber incident and a cyber incident that severely impacts an organization's essential functions. Coordinating with your partners can take many forms, depending on the needs of your organization. Examples of potential coordination include:

- Sharing information about potential threats on a dedicated Microsoft Teams channel;
- Identifying best practices to prepare for a potential threat and responding effectively and in a timely manner;
- Building a shared infrastructure (e.g., determining the best communication methods, platforms, and systems to facilitate coordination); and
- Assessing (formally or informally) your cyber gaps against the capabilities of your partners to seek out areas where you can enhance your cyber program or support your partners.

Discuss Mutual Aid

Introduction to Mutual Aid Agreements

Mutual aid agreements establish clear terms under which one party provides resources to another. These resources may include personnel, teams, facilities, equipment, and supplies, both prior to and following incidents or planned events. Mutual aid agreements provide a means for jurisdictions to augment their resources when needed to respond effectively to events or incidents that overwhelm their own capabilities. Agreements may be established between two or more jurisdictions within a state, between states, and even between nations as appropriate. Further, these agreements can be with and between private sector entities, NGOs, and other whole community partners.

Given the potential damage from cyber incidents, including cascading impacts that require consequence management, cyber mutual aid is an emerging area of interest. While emergency management mutual aid for fire, law enforcement, and emergency medical services is widely implemented, cyber mutual aid is more elusive.

In California, statewide mutual aid is voluntary aid provided between and among local jurisdictions and the state under the terms of the California Disaster and Civil Defense Master Mutual Aid Agreement enacted in 1950, now known simply as the California Master Mutual Aid Agreement (MMAA). The MMAA creates a formal structure wherein each jurisdiction retains control of its own facilities, personnel, and resources, but may also receive or render assistance to other jurisdictions within the state. In accordance with the MMAA, local and state emergency managers have responded in support of each other under a variety of plans and procedures.

Cal OES Standardized Emergency Management System (SEMS) is the cornerstone of California's emergency response system and the fundamental structure for the response phase of emergency management. The system unifies all elements of California's emergency management community into a single integrated system and standardizes key elements. SEMS facilitates priority setting, interagency cooperation, and the efficient flow of resources and information. Within and across counties, SEMS creates a framework for administering mutual aid.

The California Emergency Services Act 2015 Edition requires SEMS for managing multiagency and multijurisdictional responses to emergencies in California. State agencies and local government entities are required to use SEMS to be eligible for any reimbursement of response-related costs under the state's disaster assistance programs.

Table 3 includes general types of mutual aid agreements that jurisdictions may consider in line with the National Incident Management System (NIMS). NIMS is a comprehensive, national approach to incident management which can be applied at all levels of government. Mutual aid agreement information is reviewed in detail within the NIMS Guideline for Mutual Aid. Given the situation, different types of agreements with varied partners may be needed to ensure access to sufficient resources to meet anticipated needs. **Note:** this table is not comprehensive—other types of mutual aid exist but are beyond the scope of this document.

Table 3: Baseline Mutual Aid Information[2]

Mutual Aid Type	Description	Use	Example
Local Automatic Mutual Aid	▪ Permits the automatic dispatch and response of requested resources without incident-specific approvals or consideration of entity boundaries. ▪ Agreements usually serve as basic contracts between or among neighboring local entities.	▪ Local automatic mutual aid is used in acute situations to save lives, prevent human suffering, or mitigate property damage following an incident.	▪ A fire department from a military installation responds to an automobile accident outside of its gate because it is the closest appropriate emergency resource, even though the accident technically occurred outside the fire department's area of responsibility.
Local Mutual Aid	▪ Involves a formal request for assistance and generally covers a larger geographic area than local automatic mutual aid agreements do.	▪ Local resources may be used to assist federal departments and agencies in fulfilling their missions and special circumstances, and vice versa. ▪ May also incorporate private sector, NGO, and community-/faith-based organizations into the mutual aid network, providing parties with access to significant additional resources.	▪ Utility companies, whether privately or publicly owned, typically enter into mutual aid agreements with local communities.
Regional, Intrastate, or Statewide Mutual Aid	▪ Regional mutual aid agreements are established between multiple jurisdictions that are often sponsored by a council of governments or a similar regional body, such as a UASI. ▪ Statewide/intrastate mutual aid agreements are often coordinated through the state and incorporate both state and local governmental and nongovernmental assets in an attempt to increase preparedness statewide.	▪ These approaches are designed to help reduce the number of local and jurisdiction-to-jurisdiction mutual aid agreements. ▪ In some instances, state law requires participation in an intrastate mutual aid system.	▪ The California Fire Service and Rescue Emergency Mutual Aid Plan provides a practical and flexible pattern for the orderly development and operation of mutual aid on a voluntary basis between cities, cities and counties, fire districts, special districts, county fire departments, and applicable state agencies.

[2] U.S. Department of Homeland Security Publication 10-15, *National Incident Management System Guideline for Mutual Aid*, November 2017

NIMS mutual aid agreement guidance does not provide legal authority or direction but is intended to be used as a guideline for the development, revision, and synchronization of effective mutual aid agreements. This will ensure that jurisdictions can effectively integrate with one another prior to, during, and immediately following a large-scale incident or event. Mutual aid discussions and agreements should be developed in accordance with existing Cal OES resource management processes. For more information on California's resource sharing pathways, to include mutual aid, mission ready packages, and federal support, please see Cal OES ESF 18 Cybersecurity Annex Attachment H: Resource Sharing Guidance.

Develop a Cyber Mutual Aid Approach Among IT, Emergency Management, and County Leadership

Those driving the cyber posture within the county should engage actively with relevant stakeholders to set the county strategy. We recommend holding a meeting to get to know all relevant stakeholders and coordinate to develop a path forward. At a minimum, these meetings should include leadership from IT (CISO/CIO) and directors of emergency management departments from across the county, as well as other key leadership (e.g., city and county managers). These meetings may provide a forum for all parties to develop an approach for cyber mutual aid, as well as more informal discussions around resource and information sharing. The nature of cyber mutual aid programs will vary by county, based on specific needs and capabilities.

Cyber Planning and CIRT

Since organizations have varying cyber needs and capacity, CIRTs may look vastly different from entity to entity. A CIRT may consist of one person leading the charge, or an internal multi-disciplinary team at the ready. Depending on the scale of a cyber incident, efforts may involve partners. For instance, key team roles may be filled by local/city, operational area, state, or regional IT cybersecurity departments, system operators, legal teams, compliance officers, human resources staff, and public affairs or media relations staff.

To ensure the best possible cyber response and recovery efforts, organizations should establish clearly defined CIRT roles and responsibilities within their cyber plans. In our analysis of the Bay Area Cyber Preparedness Survey, we found that those organizations with the highest confidence in their cyber capabilities had formal, written cyber plans as well as someone in the organization's leadership dedicated to cybersecurity.

Cyber planning and dedicated cybersecurity leadership can help organizations respond quickly by streamlining decisions, outlining processes, and defining appropriate use of the technologies available. Given that 47% of Bay Area respondents did not have a cyber plan and 42% did not have anyone in leadership designated to cybersecurity (**Figure 6**), there are opportunities to improve capabilities through cyber planning. This is especially critical in organizations with a single member or small CIRT.

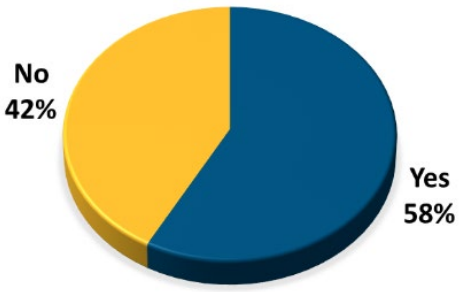

Figure 6: Bay Area aggregated response to "Does your jurisdiction/organization have an individual dedicated to cybersecurity represented among senior leadership (e.g., CISO, CIO, CSO)?"

Larger organizations may have more robust cyber capabilities, with dozens of staff assigned to CIRT response and crisis management roles. These CIRTs might have a tiered structure, such as an initial response team, a wider steering committee, and a full CIRT. This structure offers a flexible approach to ensure the response effort matches

the needs of each incident.[3] Smaller organizations may not have as many positions, with a limited number of individuals performing more than one role and no tiering available.

External Cyber Incident Response Resources

Cybersecurity services involving detection and response may be procured through service level agreements and coverage such as cyber insurance. A cyber insurance policy is designed to help an organization mitigate risk exposure by offsetting costs involved with recovery after a cyber-related security breach or similar incident.

Local governments of all sizes are continually responding to cyberattacks. Since no system is 100% secure, in addition to the full complement of cybersecurity actions, jurisdictions should consider obtaining cyber insurance. Coverage can include such items as:

- Overtime for cyber responders
- Lost revenue
- Cost of external support
- Cost of free credit monitoring
- Equipment replacement
- Legal fees
- Forensics
- Crisis management and post-event related expenses

Cal OES Incident Response Team

Cal OES, through Cal-CSIC, is the lead agency responsive for establishing and maintaining the Incident Response Team (IRT) to detect, report, and respond to cyber incidents. The state-level IRT is comprised of agencies from each of the designated four lines of effort (i.e., threat response, asset response, intelligence support, and affected entity response). The full list of response agencies is included in the Cal OES ESF 18 Cybersecurity Annex.

As outlined above in **Figure 5**, the NCRIC will notify Cal-CSIC to report situational information and request further resources to assist an affected entity, as needed. During the initial conference between the affected entity and Cal-CSIC, Cal-CSIC will determine the appropriate membership of the IRT and activate members accordingly. The IRT will report to Cal-CSIC and performs tasks as mandated by Cal-CSIC, CA-ESF 18, and the affected entity, and refers directly to Cal-CSIC for any decision-making needs.

Cal-CSIC may support response to cyber incidents occurring within non-state entities, *if requested and if resources are available to support*. The following conditions and actions are associated with assistance to non-state entities:

- Monitor the status of the external, non-state entity's cyber incident throughout the event lifecycle.

[3] American Public Power Association 6-11, *Public Power Cyber Incident Response Playbook,* August 2019

- Provide Cal OES and state leadership periodic updates on the external, non-State entity's cyber incident and whether any aspects of it are, can, and/or may adversely affect California digital technologies, systems, operations, or services.
- Initiate the recommendation for IRT stand up if the external, non-state entity's cyber incident reaches a point where it adversely affects California digital technologies, systems, operations, or services up to Severity Level 2 (Medium) or higher.

For more specific information on cyber incident response capabilities provided by the State of California, see the Cal OES ESF 18 Cybersecurity Annex.

APPENDIX A: NIST FRAMEWORK GUIDANCE

NIST Framework Core

Jurisdictions can use a set of cybersecurity activities (NIST Framework Core) to organize their activities and outcomes. The NIST Framework Core reflects cybersecurity industry standards and best practices in a way that enables communication about cybersecurity activities and outcomes across an organization. The NIST Framework Core is comprised of five functions: Identify, Protect, Detect, Respond, and Recover. If an organization considers and assesses against these five functions, it enables them to obtain a strategic-level understanding of their cybersecurity risk (**Table 4**). The NIST Framework Core is available on NIST's website at https://www.nist.gov/cyberframework/nist-cybersecurity-framework-csf-reference-tool.

The NIST Framework Core does not provide organizations with a checklist of actions to perform or a prescriptive plan for updating and enhancing their cybersecurity programs. Instead, it presents key cybersecurity outcomes that are helpful in managing and mitigating cybersecurity risk, along with example guidance that can help to achieve those outcomes. The functions should be performed concurrently and continuously to form an operational culture capable of managing the constantly evolving cyber threat environment.

Table 4: NIST Framework Functions

Function	Description
Identify	Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities
Protect	Develop and implement appropriate safeguards to ensure delivery of critical services
Detect	Develop and implement appropriate activities to identify the occurrence of a cybersecurity event
Respond	Develop and implement appropriate activities to take action regarding a detected cybersecurity incident
Recover	Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident

The NIST Framework Core also identifies underlying key categories and subcategories for each function and matches them with informative references as shown in **Figure 7**.

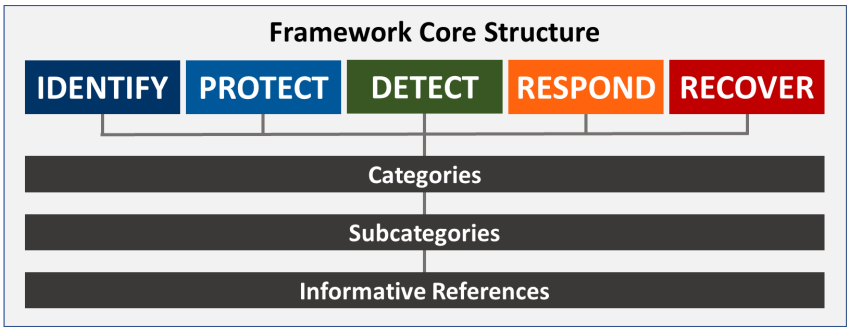

Figure 7: Framework Core Structure

Categories are subcomponents of a function that reflect groups of cybersecurity outcomes that are related to cybersecurity program requirements and specific activities (e.g., Identity Management and Access Control, Governance, Risk Management). Subcategories break down a category into even more specific outcomes from technical or management activities (e.g., risk responses are identified and prioritized; external information systems are catalogued; response and recovery plans are tested). The subcategories identify a set of results to help organizations to achieve the outcomes in each category.

Lastly, informative references list the specific sections of various cybersecurity standards, guidelines, and practices that may help your organization to better understand how to achieve the outcomes associated with each subcategory. Refer to NIST or the Bay Area Cyber Toolkit for a full list of all NIST Framework Core categories and subcategories, along with the informative references for each. Your organization should use this resource to better understand your cybersecurity risk and where you may have gaps.

While these informative references are not exhaustive—and you should feel free to refer to other relevant guidance—they are based upon frequently used, cross-sector resources that have proven to be helpful to many organizations.

NIST Framework Tiers

Tiers describe the level of sophistication of an organization's cybersecurity risk management practices. Ranging from Tier 1 to Tier 4, the tiers help organizations to provide context on how they view their own cybersecurity risk and the processes they have established to manage it. Tiers can also help organizations determine and communicate the extent to which their cybersecurity processes are informed by business needs and how well they are integrated into the organization's overall risk management. Refer to **Table 5** for a definition of each tier, organized by three assessment categories: risk management process, integrated risk management program, and external participation.

Table 5: NIST Implementation Tiers

Tier	Definition
Tier 1 – Partial	**Risk Management Process:** Organizational cybersecurity risk management practices are not formalized, and risk is managed in an ad hoc and sometimes reactive manner.
	Integrated Risk Management Program: There is limited awareness of cybersecurity risk at the organizational level.
	External Participation: The organization does not understand its role in the larger ecosystem with respect to either its dependencies or dependents.
Tier 2 - Risk Informed	**Risk Management Process:** Risk management practices are approved by management but may not be established as organizational-wide policy.

Tier	Definition
	Integrated Risk Management Program: There is an awareness of cybersecurity risk at the organizational level, but an organization-wide approach to managing cybersecurity risk has not been established.
	External Participation: Generally, the organization understands its role in the larger ecosystem with respect to either its own dependencies or dependents, but not both.
Tier 3 – Repeatable	**Risk Management Process:** The organization's risk management practices are formally approved and expressed as policy.
	Integrated Risk Management Program: There is an organization-wide approach to manage cybersecurity risk.
	External Participation: The organization understands its role, dependencies, and dependents in the larger ecosystem and may contribute to the community's broader understanding of risks.
Tier 4 – Adaptive	**Risk Management Process:** The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators.
	Integrated Risk Management Program: There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events.
	External Participation: The organization understands its role, dependencies, and dependents in the larger ecosystem and contributes to the community's broader understanding of risks.

The tier selection process considers an organization's current risk management practices, threat environment, legal and regulatory requirements, information sharing practices, business or mission objectives, supply chain cybersecurity requirements, and organizational constraints. Organizations should work to identify the tier that they want to build towards, while ensuring that the identified tier is feasible to implement given available resources. It should also meet the organization's goals for the acceptable level of cybersecurity risk. When determining the desired tier, organizations should consult external guidance from a variety of sources, including the Federal Government, Multi-State Information Sharing and Analysis Center (MS-ISAC), information sharing and analysis organizations, and existing cybersecurity program maturity models.

As described above, each function is organized with categories and subcategories that guide jurisdictions in evaluating the status of their cybersecurity program elements. By working their way through each category and subcategory, organizations will be more informed about their cybersecurity posture and will be better able to identify what tier they currently fall under. Then, through a risk-based review, organizations can compare their current tier with their desired tier to identify what gaps exist in their cybersecurity program. This gap analysis can then be used to help organizations understand what they need to do to progress to a desired tier.

Tiers are meant to support organizational decision-making about how to manage cybersecurity risk, as well as which dimensions of the organization are higher priority and could receive additional resources. This is not a one-size-fits-all approach and tier selection does not correlate to the maturity of a cybersecurity program. Rather, it reflects a cost-benefit analysis by each jurisdiction to determine a feasible tier that provides cost-effective reductions in cybersecurity risk. Ultimately, successful implementation of the NIST Framework is based upon achieving the outcomes described in the organization's Target Profile through the application of concepts such as tiers.

Each jurisdiction must determine its own level of acceptable risk and ability to manage that risk. Jurisdictions across the Bay Area will vary in their tier selections based on their risk tolerance and available resources.

NIST Framework Profile

The NIST Framework Profile provides a way to align the functions, categories, and subcategories with your organization's business requirements, level of risk tolerance, and available resources. A Profile enables organizations to establish a roadmap for reducing cybersecurity risk that is aligned with organizational and sector goals, considers legal or regulatory requirements and industry best practices, and reflects risk management priorities. Organizations can use the Profile(s) they develop as a tool for identifying opportunities for improvement in their cybersecurity posture. Organizations with a complex make-up may choose to develop multiple Profiles that are aligned with organizational components to ensure that they recognize each component's individual needs.

The NIST Framework does not prescribe a particular format or template for the Profile, so there is no "right" or "wrong" way to create or use them.

One common way for an organization to develop a Profile is to map cybersecurity requirements, mission objectives, and operating methodologies, along with current practices against the NIST Framework subcategories. This results in a "Current-State Profile" that outlines the cybersecurity outcomes presently being achieved. This Current-State Profile can serve as an "executive summary" of what you learned about your organization through the previous aspects of the NIST Framework described above.

Profiles can also be used to describe the desired target state of specific cybersecurity activities. An organization can compare their Current-State Profile against a Target Profile. In doing so, the organization can observe gaps in their cybersecurity posture and identify opportunities for improvement. From the gap analysis, jurisdictions can develop an action plan to reach the desired Profile and reduce cybersecurity risk.

Ideally, organizations will outline how they plan to address their gaps to fulfill a given category or subcategory. The priority, size of gap, and estimated cost of the corrective actions help organizations plan and budget for cybersecurity improvement activities. Since each jurisdiction is unique with respect to its inherent capabilities and resources, each will identify unique solutions based on its level of acceptable risk in a cost-effective, prioritized manner as highlighted in **Figure 8** examples.

Subcategory *(Examples)*	Priority of Outcome	Gaps Relative to Subcategory Outcome	Budget	Actions to Close Gap (Year 1)	Actions to Close Gap (Year 2)	Actions to Close Gap (Year 3)
Incident alert thresholds are established	Moderate	Small	$	[Describe Action]	[Describe Action]	[Describe Action]
Communications and control networks are protected	Moderate	Large	$$$	[Describe Action]	[Describe Action]	[Describe Action]
Backups of information are conducted, maintained, and tested	High	Medium	$$	[Describe Action]	[Describe Action]	[Describe Action]

Figure 8: Example of a Basic Target Profile

These Profiles can be an extremely effective way to communicate your current and target cybersecurity capabilities and risk to your partners and stakeholders, including your own leadership and vendors. This enhanced coordination can help your organization make progress towards closing your identified gaps to build a more comprehensive and effective cybersecurity program.

NIST Framework Implementation Coordination

The success of a cybersecurity program begins at the top of an organization and works with the various levels in a cyclical fashion as shown in Figure 9.

As noted in the Bay Area UASI Cyber Preparedness Survey, respondents had higher confidence in their organization's cyber posture when they had a senior leader dedicated to cybersecurity.

The executive level establishes priorities based on available resources and overall risk tolerance to the organization's business/process level. The business/process level works with the implementation/operations level to establish operational needs and create the organization's Profile. The implementation/operations level executes Profile implementation and provides associated feedback. The business/process level uses the feedback to conduct an impact assessment and reports the results to the executive level, informing the ongoing risk management process.

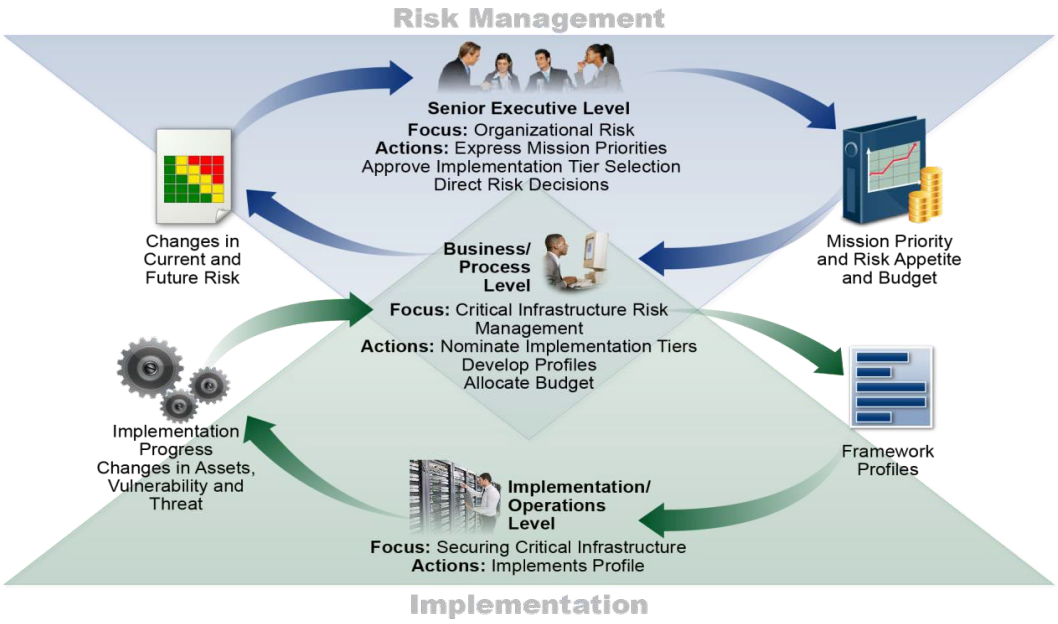

Figure 9: NIST Framework Implementation

Implementing the NIST Framework

While the NIST Framework does not replace an organization's cybersecurity program, it may be used to supplement the existing cybersecurity program (or build a new one) to identify, access, and manage cybersecurity risk. In particular, by establishing a profile using the NIST Framework Core, jurisdictions can identify critical activities and prioritize expenditure to maximize the impact of the cybersecurity budget. In addition, the NIST Framework can help jurisdictions communicate cybersecurity requirements to citizens, vendors, external partners, and others.

As jurisdictions improve or build new cybersecurity programs, they may use the NIST Framework throughout the plan, design, build/buy, deploy, operate, and decommission life cycle. Jurisdictions can use the outcomes from their Target Profile as the basis for ongoing cybersecurity operations. Based on the Current-State Profile, jurisdictions can determine how well they are achieving desired outcomes in the NIST Framework Core functions. Results can range from determining the organization is overinvesting to achieve outcomes, to meeting desired outcomes, to having cybersecurity gaps.

Cybersecurity Program Development or Improvement

Repeat the following step as necessary in a planning and continuous improvement process:

1. **Prioritize and Scope.** Each jurisdiction can adapt the NIST Framework to support its unique operational lines or processes. Each operational line of the jurisdiction may have different needs and associated risk tolerance. Risk tolerances may be reflected in a target tier.
    a. Identify operational/mission objectives and high-level jurisdictional priorities.
    b. Make strategic decisions regarding cybersecurity implementations and determine the scope of systems and assets that support the selected operational line or process.
2. **Orient.** Once the scope of the cybersecurity program has been determined for the operational line or process, the jurisdiction should:
    a. Identify related systems and assets, regulatory requirements, and overall risk approach.
    b. Consult sources to identify threats and vulnerabilities applicable to those systems and assets.

It is important to identify emerging risks and use cyber threat information from internal and external sources to gain a better understanding of the likelihood and impact of cybersecurity events.

3. **Create a Current-State Profile.** Develop a Current-State Profile by indicating which category and subcategory outcomes from the NIST Framework Core are currently being achieved. If an outcome is partially achieved, noting this fact will help support subsequent steps by providing baseline information.
4. **Conduct a Risk Assessment.** This assessment could be guided by the organization's overall risk management process or previous risk assessment activities.
    a. Analyze the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization.

5. **Create a Target Profile.** Create a Target Profile that focuses on the assessment of the NIST Framework categories and subcategories describing the organization's desired cybersecurity outcomes.

    a. Jurisdictions may develop their own additional categories and subcategories to account for unique organizational risks.

    b. Consider influences and requirements of external stakeholders such as sector entities, citizens, and partner jurisdictions or organizations when creating a Target Profile.

    c. The Target Profile should appropriately reflect criteria within the target tier.

Using Target Profiles encourages organizations to make informed decisions about cybersecurity activities, supports risk management, and enables them to perform cost-effective, targeted improvements.

6. **Determine, Analyze, and Prioritize Gaps.** The jurisdiction compares the Current-State Profile and the Target Profile to determine gaps.

    a. Create a prioritized action plan to address gaps—reflecting mission drivers, costs and benefits, and risks—to achieve the outcomes in the Target Profile.

    b. Determine resources, including funding and workforce, necessary to address the gaps.

7. **Implement Action Plan.** The jurisdiction determines which actions to take to address the gaps, if any, identified in the previous step and then adjusts its current cybersecurity practices in order to achieve the Target Profile.

    a. Jurisdictions should determine which standards, guidelines, and practices—including those that are sector specific—work best for their needs.

Jurisdictions repeat the steps as needed to continuously assess and improve its cybersecurity. More frequent repetition of the orient step may improve the quality of risk assessments. To monitor progress, jurisdictions can develop iterative updates to the Current-State Profile, subsequently comparing the Current-State Profile to the Target Profile.

This page intentionally left blank

APPENDIX B: BAY AREA CYBER PREPAREDNESS SURVEY METHODOLOGY AND ANALYSIS

As introduced in the Bay Area Region-wide Cyber Preparedness section, the Bay Area UASI participated in a 2019 survey of six key focus areas, including planning, incident response, resources, training and exercises, and threat landscape. This appendix provides additional details of the methodology used to analyze the survey results and highlight several interesting findings beyond those summarized above.

Methodology

Analysis of the survey results divided the participants into two distinct groups. The most significant differences between the two groups are described below. In general, the groups differed around resources, planning, personnel, and confidence. The grouping was used to identify the questions which most sharply differentiated the participants from one another. It was initially observed that the answers on some survey questions appeared highly correlated with others. To confirm this subjective observation, this analysis converted the multiple choice and "on a scale of 1-5" answers into a numerical matrix and calculated the significant correlations.

Results

Given the high correlation between the "on a scale of 1-5" answers, they were combined into an average "confidence score" to condense the results. Analyzing the survey answers for maximum variance, it was found that there seemed to be two distinct participant groups. While Group 2 participants tended to have an individual dedicated to cybersecurity in senior leadership, Group 1 participants tended not to have one. Similar variations were noted on themes of budget, resources, planning, and mutual aid.

Within the **Figure 10** charts—which depict the impact on confidence that participants have in their cybersecurity program—several interesting results stood out, including:

- Organizations with an individual dedicated to cybersecurity in senior leadership had more confidence in their organization's cybersecurity posture.
- Organizations with a cyber plan in place had greater confidence in their cyber response.
- Those participants having a process for engaging in mutual aid with external stakeholders were far more likely to have confidence in their cybersecurity posture.

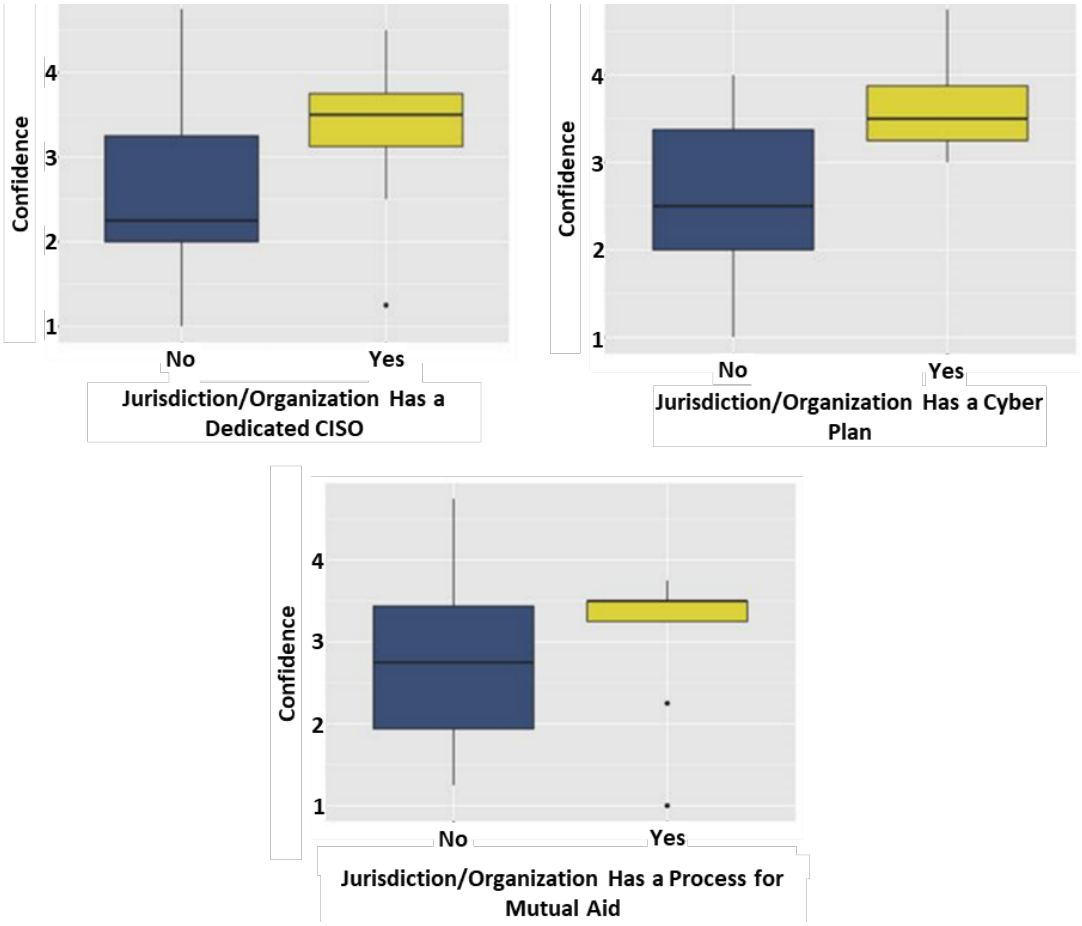

Figure 10: Confidence Results – Dedicated CISO, Cybersecurity Plan, and Process(es) for Mutual Aid

As demonstrated in **Figure 11**, organizations with a higher budget (shown by their percentile rank) generally had a greater confidence. Increased budgets can manifest in larger workforce and increased technologically capacity. Budget by itself, however, was not always predictive. For example, the participant with the highest confidence score was only at the 60th percentile for budget. One important note on this question is that it does not have a baseline of the overall organizational budget—it focuses solely on organization's cyber budget allocations.

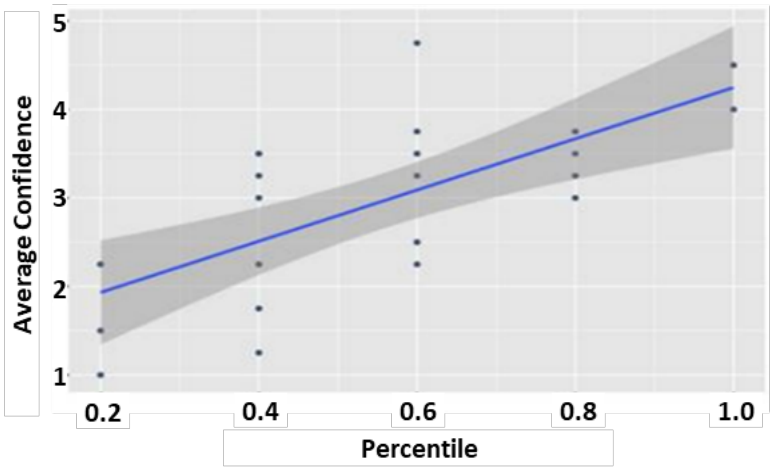

Figure 11: Cyber Budget

APPENDIX C: BAY AREA CYBERSECURITY TRAINING OPTIONS

Training is a critical piece of a comprehensive cyber incident response capability. There are several areas Bay Area organizations should consider when establishing or updating their training programs.

Baseline Cybersecurity Training

In the 2019 Bay Area UASI Cyber Preparedness Survey, nearly 1 in 5 respondents cited a lack of cybersecurity training as one of their top three resources challenges related to cyber preparedness (**Figure 12**). Investing in cybersecurity, including effective baseline training, is a sound best practice that can have an impressive return on investment.

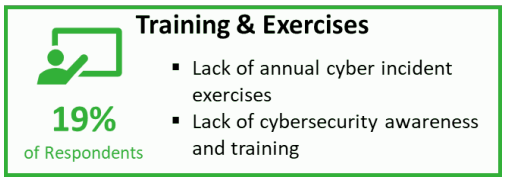

Figure 12: Lack of cybersecurity awareness and training was a significant shortfall indicated by Bay Area respondents

Organizations should consider implementing basic cybersecurity training and requiring employees to refresh their understanding every year. Many private sector organizations and NGOs provide enterprise cybersecurity awareness training. Be sure to choose a reputable source. As a jumping off point, check out NIST's National Initiative for Cybersecurity Education page to review free and low cost cybersecurity online content.

Cyber Planning Training Courses

To cultivate the strongest cyber incident response capabilities, organizations across the Bay Area should engage in cyber planning during steady state. Having established relationships with key partners in addition to standard operating procedures, plans, and policies will help mitigate potential damage from cyberattacks. As part of its current Cyber Project, the Bay Area UASI in coordination with the NCRIC developed a Cyber Toolkit to help organizations begin or update their cyber planning. Associated information, including a recorded training, is included below. We have also provided recommendations for additional cybersecurity planning courses within this section.

Bay Area UASI Cyber Toolkit Training

The Bay Area Cyber Toolkit is designed to help you develop cybersecurity planning that enables your organization to quickly identify, respond to, and recover from cyber incidents. The Cyber Toolkit materials have been finalized and uploaded to the Bay Area UASI website. We encourage you to download these materials and share them with stakeholders within your organization and any partners you think may find them useful.

The Bay Area UASI offers a recorded training or PowerPoint slides to review the Cyber Toolkit and offer guidance on how best to engage with its contents, including:

- **Cyber Toolkit Executive Summary:** Introduces and describes the contents of the Cyber Toolkit and explains the relationships between the plan templates and other related planning efforts.
- **Technology Recovery Plan Template:** Identifies priorities, strategies, and resources that your organization/jurisdiction can use when recovering from a cyber incident.

- **Cyber Incident Response Plan Template:** Provides the guidance and structure needed to develop a clear and actionable plan for your organization/jurisdiction to implement quickly in response to an actual or suspected cyber incident.

Bay Area Training & Exercise Program

Training and exercises are critical means to attain, practice, validate, and improve emergency response and preparedness capabilities. The Bay Area Training & Exercise Program (BATEP) offers training and exercise opportunities, inclusive of community preparedness, supporting whole community partners throughout the Bay Area 12-county region in addressing natural and human-caused threats and hazards. To register for a training course, or for more information see www.batep.org.

Additional Cybersecurity Planning Courses

Beyond the Bay Area Cyber Toolkit Training, see **Table 6** for more recommended courses addressing cybersecurity planning.

Table 6: Cybersecurity Planning Courses

Course	Offered By	Description	Length
AWR353 Developing a Community Cyber Security Program	Texas A&M Engineering Extension Service (TEEX)	This course will introduce students to the DHS-supported Community Cyber Security Maturity Model (CCSMM) which can be used as a guide for communities and states in developing their own CCSMM-consistent cyber security programs. Students will learn what is required to develop a coordinated, sustained, and viable community cyber security program and resources available to assist in improving awareness, information sharing, policies, and plans.	2 hours
AWR366 Developing a Cybersecurity Annex for Incident Response	TEEX	At the end of this course, participants should possess the fundamentals needed to design and develop a cyber annex for SLTTs. It addresses what the annex is, how it is used, who should participate in the design, implementation, and execution.	2 hours
IS-523: Resilient Accord – Exercising Continuity Plans for Cyber Incidents	Emergency Management Institute (EMI)	The course is to increase continuity of operations awareness and discuss how to execute continuity operations during a cyber security event.	3 hours

Emergency Management Training for Cyber Professionals

In the 2019 Bay Area UASI Preparedness Survey, 69% of respondents were unsure or responded that their organization's cyber leadership *did not* receive emergency management training (**Figure 13**). Given that cyberattacks may have cascading impacts that result in consequence management, it is critical for cyber and emergency management professionals to coordinate effectively during cyber incident response. **Table 7** includes recommended foundational courses offered through the Federal Emergency Management Agency's (FEMA) EMI Independent Study (IS) Program.

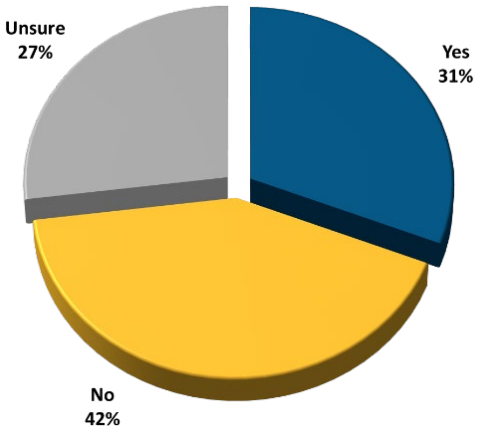

Figure 13: Bay Area aggregated response to "Does your jurisdiction/organization's cyber leadership receive emergency management training?"

Table 7: Recommended Emergency Management Courses

Course	Description	Length
IS-100.b (ICS 100) Introduction to Incident Command System	The goal of this course is to promote effective response by familiarizing personnel with the Incident Command System (ICS) framework, and the principles used to manage incidents. This course also prepares personnel to coordinate with response partners from all levels of government and the private sector.	2 hours
IS-200.b (ICS 200) ICS for Single Resources and Initial Action Incidents	This course review reviews ICS, provides the context for ICS within initial response, and supports higher level ICS training.	4 hours
IS-700.a National Incident Management System (NIMS), An Introduction	This course provides an overview of NIMS. NIMS defines the comprehensive approach guiding the whole community—all levels of government, NGOs, and the private sector—to work together seamlessly to prevent, protect against, mitigate, respond to, and recover from the effects of incidents. The course provides learners with a basic understanding of NIMS concepts, principles, and components.	3.5 hours
IS-703.a NIMS Resource Management Course	The goal of the NIMS Resource Management course is to introduce federal and SLTT emergency managers, first responders, and incident commanders from all emergency management disciplines to NIMS Resource Management. This includes private industry and volunteer agency personnel responsible for coordination activities during a disaster.	3.5 hours
IS-706 NIMS Intrastate Mutual Aid - An Introduction	This course introduces NIMS intrastate mutual aid and assistance. You will learn about the purpose and benefits of mutual aid and assistance. You will also learn about the emphasis that NIMS places on mutual aid and assistance. The course explains how to develop mutual aid and assistance agreements and mutual aid operational plans.	2.5 hours

Course	Description	Length
IS-800.b National Response Framework, An Introduction	The goal of the IS-0800.d, National Response Framework, An Introduction, is to provide guidance for the whole community. Within this broad audience, the National Response Framework focuses especially on those who are involved in delivering and applying the response core capabilities, including: private sector partners, NGOs, government officials, community leaders, emergency management practitioners, and first responders.	3 hours

Advanced Cybersecurity Training

For advanced cybersecurity training offerings, CISA's National Initiative for Cyber Careers and Studies Education and Training Catalog is a useful reference. The catalog offers information on over 5,000 cybersecurity-related courses for cyber professionals. CISA's Federal Virtual Training Environment (FedVTE) provides free online cybersecurity training to federal and SLTT government employees, federal contractors, and United States military veterans. FedVTE offers advanced, intermediate, and basic level courses. There are several publicly available courses requiring no log-in, and many more courses offered if you are a stakeholder identified above and set up a free log-in.

APPENDIX D: MUTUAL AID AGREEMENT CONSIDERATIONS

Development Guidance

When establishing mutual aid agreements, organizations should consider the following agreement elements, as shown in **Table 8,** to ensure clarity in the commitment, scope, and general procedures for all parties.[4] To ensure cyber incident response elements are properly addressed and included within cyber mutual aid agreements, coordinate with your CISO, CIO, and/or IT departments as appropriate. For a template on drafting a Memorandum of Understanding, see the Cyber Incident Response Plan template within the Bay Area UASI Cyber Toolkit.

Table 8: Mutual Aid Agreement Element Descriptions

Agreement Element	Description
Purpose and Scope	Identify the agreement's conditions, length, and general legal scope or effect, such as the intent to bind parties or severability. Present the reason for the agreement and identify the parties, the types of services addressed, and any applicable mutual aid service limitations. Organizations often specify whether the agreement's intent is to provide resources for declared disasters or surge capacity prior to a disaster declaration.
Benefits	Outline the economic, logistical, or other benefits that the mutual aid agreement may provide to the parties entering into the agreement. Because owning and maintaining all of the resources needed to respond to extreme or high-demand incidents is cost-prohibitive for most communities, entering into mutual aid agreements provides economic and logistical efficiencies to support any gaps in resources and capability.
Authorities	Specifically state the legal basis for the parties to enter into the mutual aid agreement in an authorities section. This may include the state laws, local ordinances, tribal resolutions, regulations, or other applicable authorities.
Definitions	Define key terms in the agreement to ensure all parties share a common vocabulary, especially any terms that are specific or unique to the circumstances of the contract.
Governance Structure and Operations Oversight	The governance section should specify who is responsible for overseeing the agreement and how those personnel communicate policies and procedures to guide the agreement's implementation and operation. Being clear about the governance structure can expedite decision making, reduce the time required to request assistance, and ensure all parties understand the chain of command.

[4] U.S. Department of Homeland Security Publication 10-15, *National Incident Management System Guideline for Mutual Aid,* November 2017

Agreement Element	Description
Recognition of Licensure and Certifications	Identify licenses and certifications that qualify individuals to perform specific duties (e.g., doctors, emergency medical technicians) and ensure receiving parties recognize licensure and/or certification across geopolitical boundaries. Mutual aid agreements that cross geopolitical borders should reconcile that practitioners licensed in one political jurisdiction retain the authorization to work at the level of their license or certification in other political jurisdictions as a part of the response.
Protocol for Interoperable Communications	Pre-arranged communication frequencies and procedures are critical for effective execution. Identify the overarching requirement for ensuring the necessary level of voice and data communications.
Tort Liability Indemnification	Specify how parties will address tort liability. For mutual aid purposes, indemnifying the person or jurisdiction or holding them harmless is a way to address liability concerns.
Insurance	Address the parties' responsibilities to provide insurance coverage. Many political jurisdictions are self-insured, while private sector organizations tend to carry commercially available insurance. Mutual aid agreements often include provisions for insurance covering individuals and equipment.
Workers' Compensation	Address how parties will respond to workers' compensation coverage and claims, including those from private sector, NGO, and community-/faith-based organization employees and volunteers.
Deployment Notification	It is a best practice to include acceptable deployment notification protocols and documents in mutual aid documents to discourage unrequested resources. This section should address the documentation that will be considered official authorization to deploy or travel authorizations citing a specific purpose. Having explicit deployment notification will discourage self-deployment of unrequested resources.
Reciprocity/Reimbursement	Mutual aid agreements must specify how the receiving party will compensate the sending party. This compensation may be provided using the following structures: ▪ **In-kind agreements:** State that the party receiving services will reciprocate by providing the same type of services over time. ▪ **Equity agreements:** State that the parties will exchange equitable services, though not of an in-kind nature. The value of the services exchanged und an equity agreement is equal. ▪ **Reimbursable agreements:** Provide the terms of the exchange of services for payment. Contracts specify the costs of various types of services and the payment mechanisms parties will use. In some incidents, sending parties cannot afford to lend their services and resources for extended periods of time without reimbursement.
Termination	Specify how and when parties may terminate the agreement and the notification time period. Documenting this information minimizes cost and risk to all parties.
Dispute Resolution	Include methods and timelines for personnel to make, process, and investigate complaints, and define the dispute resolution process. This includes how personnel make formal complaints, the adjudication method, timeframes for each step, and the implementation of resolution.

Agreement Element	Description
Modification and Amendment Management	Identify the methods and timelines for the periodic review of the agreement by all parties, the process for parties to propose modifications or amendments to the document, and the process for approving changes.
Operational Plan and Procedures Requirements	Specify any requirements concerning the development of a mutual aid operational plan, including procedures, the timeline for completion, and the process for approving and implementing the plan. Typically, this includes procedures for how mutual aid resources and personnel who were mobilized to support an incident or planned event continue under the operational control of their day-to-day leaders. It often also includes details on how the receiving party's existing ICS structure integrates resources and personnel, as well as how the receiving party maintains control over the incident and makes organizational and strategic goals and objectives and tactical assignments to the mutual aid resources through the chain of command.
Supplemental Information Based on Declaration Status	Include supplemental information on authorities and procedures that are triggered under governor-declared disasters.

This page intentionally left blank

APPENDIX E: GLOSSARY AND ACRONYMS

Glossary

Availability: Assurance that the systems responsible for delivering, storing, and processing information are accessible when needed by those who need them.

Business Impact Analysis (BIA): Provides a method of identifying and evaluating the effects of various threats and hazards and the impact they may have on the ability of an organization to perform its essential functions. It facilitates the identification and mitigation of vulnerabilities to ensure that when a disruption or crisis occurs, an organization can still effectively perform essential functions. The results of the BIA will establish the foundation for evaluating and establishing risk mitigation strategies, which ensure the continued performance of all organizational essential functions.

Business Process Analysis (BPA): A systematic process that identifies and documents the activities and tasks that are performed within an organization. A BPA captures and maps the functional processes, workflows, activities, subject matter expertise, systems, resources, controls, data, and facilities required in the execution of a function or task.

Chief Information Officer (CIO): An executive job title commonly given to the person at an enterprise in charge of information technology (IT) strategy and the computer systems required to support the organization's unique objectives and goals.

Chief Information Security Officer (CISO): The executive responsible for an organization's information and data security.

Continuity of Operations (COOP): An effort within individual executive departments and agencies to ensure that Primary Mission Essential Functions (PMEFs) continue to be performed during a wide range of emergencies, including localized acts of nature, accidents and technological or attack-related emergencies.

Continuity of Operations (COOP) Plan: The documentation of a predetermined set of instructions or procedures that describe how an organization's essential functions will be sustained during and after a significant disruption.

Cyber Incident Response Team (CIRT): Individual or core team composed of subject- matter experts and information privacy and security staff that aids in protecting the privacy and security of information that is confidential by law and provides a central resource for an immediate, effective, and orderly response to cyber incidents at all levels of escalation. May also be known as an Incident Response Team (IRT).

Cyber Insurance: Cyber insurance is designed to help an organization mitigate risk exposure by offsetting costs involved with recovery after a cyber-related security breach or similar incident.

Data: Information in an oral, written, or electronic format that allows it to be retrieved or transmitted.

Emergency Management: The organization and management of the resources and responsibilities for dealing with all aspects of emergencies (preparedness, response, mitigation, and recovery).

Event: An observable occurrence on a network or system or of confidential information.

Hardware: The physical technology used to process, manage, store, transmit, receive, or deliver information. The term does not include software. Examples include laptops, desktops, tablets, smartphones, thumb drives, mobile storage devices, CD-ROMs, and access control devices.

Incident: An attempted or successful unauthorized access, use, disclosure, exposure, modification, destruction, release, theft, or loss of sensitive, protected, or confidential information or interference with systems operations in an information system.

Information Security: The administrative, physical, and technical protection and safeguarding of data (and the individual elements that comprise the data).

Integrity: Assurance that the data are authentic, accurate, and complete and can be relied upon to be sufficiently accurate for their purpose.

Mutual Aid: The timely and efficient sharing of capabilities in the form of resources and services upon request.

Mutual Aid Agreement: A written or oral agreement between and among agencies/organizations and/or jurisdictions that provides a mechanism to quickly obtain assistance in the form of personnel, equipment, materials, and other associated services. The primary objective is to facilitate the rapid, short-term deployment of emergency support prior to, during, and/or after an incident.

NIST Framework: The NIST Framework integrates industry standards and best practices to help organizations manage their cybersecurity risks. It provides a common language that allows staff at all levels within an organization—and at all points in a supply chain—to develop a shared understanding of their cybersecurity risks. The Framework not only helps organizations understand their cybersecurity risks (threats, vulnerabilities and impacts), but how to reduce these risks with customized measures. The Framework also helps them respond to and recover from cybersecurity incidents, prompting them to analyze root causes and consider how they can make improvements.

Northern California Regional Intelligence Center (NCRIC): The NCRIC is the Bay Area's nationally renowned "All Crimes Fusion Center" staffed, operated, and managed by representatives from local public safety agencies in the region with oversight from the Northern California High Intensity Drug Trafficking Area (NCHIDTA) Executive Board. The NCRIC provides regional analytical and investigative support to local, state and federal law enforcement agencies involving terrorism, cybersecurity, information sharing, risk management and infrastructure protection.

Recovery: Process of recreating files which have disappeared or become corrupted from backup copies.

Risk Management: Process for identifying, analyzing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level considering associated costs and benefits of any actions taken.

Sensitive Data: While not necessarily protected by law from use or disclosure, data that is deemed to require some level of protection as determined by an individual agency's standards and risk management decisions. Some examples of "Sensitive Data" include but are not limited to operational information, personnel records. information security procedures., internal communications, and Information determined to be authorized for use or disclosure only on a "need-to-know" basis.

Threat: Any circumstance/event with the potential to adversely impact an information system through the unauthorized access, destruction, disclosure, modification of data and/or denial of service.

Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited.

Acronyms

Refer to **Table 9** for definitions of all acronyms used in this Framework.

Table 9: Acronym List

Acronym	Definition
BATEP	Bay Area Training & Exercise Program
BIA	Business Impact Analysis
BPA	Business Process Analysis
Ca-ESF 18	California Emergency Support Function 18
Cal-CSIC	California Cybersecurity Integration Center
Cal OES	California Governor's Office of Emergency Services
CCSMM	Community Cyber Security Maturity Model
CFTF	Cyber Fraud Task Force
CIO	Chief Information Officer
CIOCC	CISA Integrated Operations Coordination Center
CIRP	Cyber Incident Response Plan
CIRT	Cyber Incident Response Team
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
COG	Continuity of Government
COOP	Continuity of Operations
CRWG	Cybersecurity Resilience Work Group
CTF	Cyber Task Force
DHS	Department of Homeland Security
EA	Essential Assets
EF	Essential Functions
EMI	Emergency Management Institute
EMMA	Emergency Management Mutual Aid
ESF	Emergency Support Function
FBI	Federal Bureau of Investigations
FedVTE	Federal Virtual Training Environment
FEMA	Federal Emergency Management Agency
ICS	Incident Command System
IRT	Incident Response Team

Acronym	Definition
IS	Independent Study
IT	Information Technology
MMAA	Master Mutual Aid Agreement
MMAC	Master Mutual Aid Compact
MS-ISAC	Multi-State Information Sharing & Analysis Center
NCATS	National Cybersecurity Assessments and Technical Services
NCCIC	National Cybersecurity & Communications Integration Center
NCHIDTA	Northern California High Intensity Drug Trafficking Area
NCRIC	Northern California Regional Intelligence Center
NCSR	Nationwide Cybersecurity Review
NGO	Non-governmental Organization
NIMS	National Incident Management System
NIST	National Institute of Standards and Technology
PIO	Public Information Officer
RFC	Regional Fusion Center
SEMS	Standardized Emergency Management System
SLTT	State, Local, Tribal, and Territorial
STAC	State Threat Assessment Center
TEEX	Texas A&M Engineering Extension Service
TRP	Technology Recovery Plan
UASI	Urban Areas Security Initiative Program