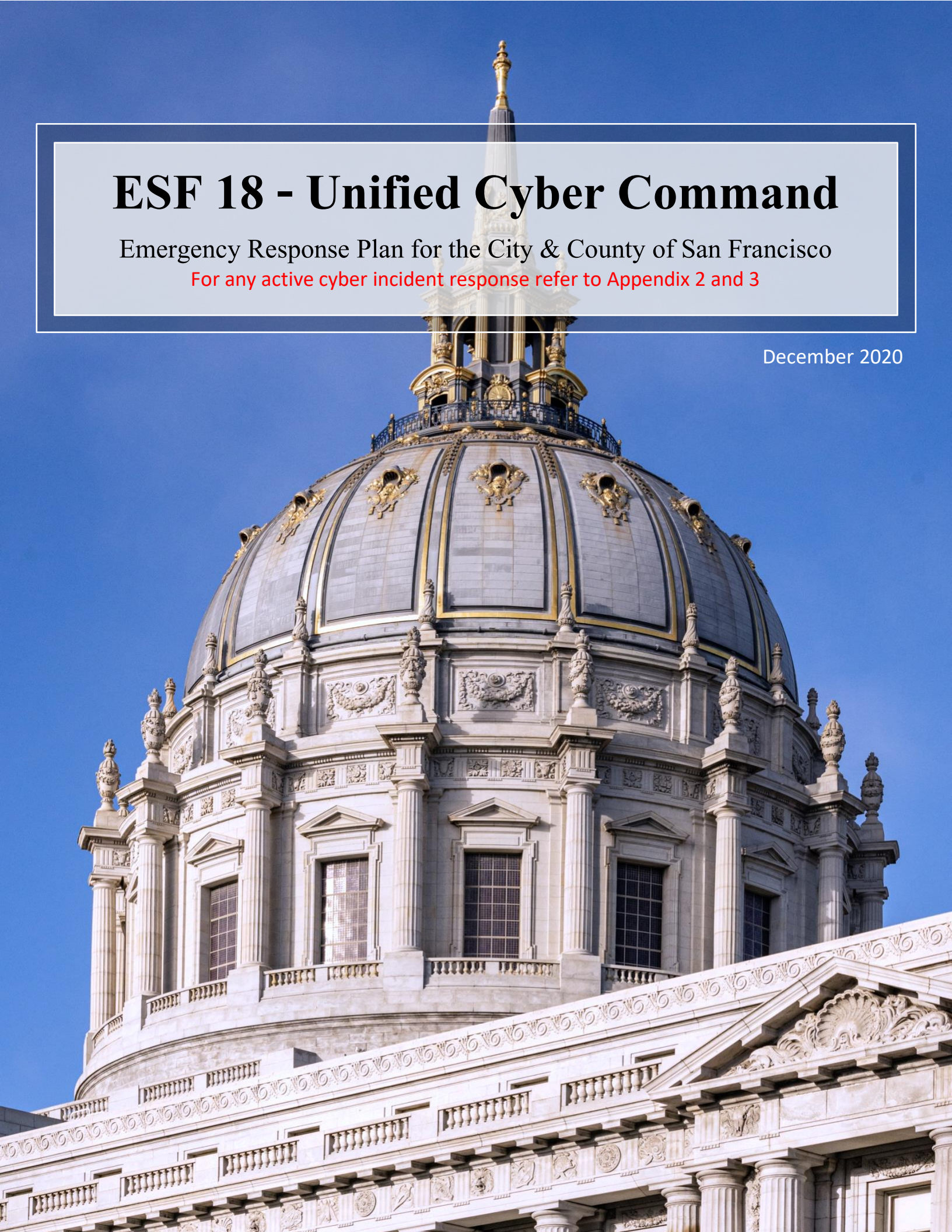


ESF 18 - Unified Cyber Command

Emergency Response Plan for the City & County of San Francisco

For any active cyber incident response refer to Appendix 2 and 3

December 2020

Executive Summary

To ensure City resilience during a severe cyberattack and to enable a successful restoration of City services, a new ongoing program called San Francisco Unified Cyber Command has been initiated. This program supports the Citywide cybersecurity policy that was adopted by the Committee on Information Technology (COIT) in June 2018 and mandates Departmental risk mitigation and alignment with city requirements (https://sfcoit.org/cybersecurity).

The Department of Emergency Management (DEM) and the Department of Technology (DT), in partnership with all City departments developed and finalized San Francisco Unified Cyber Command plan - Emergency Support Function 18 (ESF 18). ESF 18 will be added to the City Emergency Response Plan.

Operational checklists in Appendix 2 and 3 of the ESF 18 plan provide step-by-step protocols for Departments to use during a data breach or a cyberattack.

Department Heads are asked to support SF Unified Cyber Command by:

1. Reviewing published ESF 18 plan to understand department responsibilities and protocols.
2. Developing a department-specific cyber appendix to your Continuity of Operations Plan (COOP) that links your cyber incident response with the SF Unified Cyber Command plan. A template available in Appendix 4.
3. Planning and conducting annual exercise of department-specific cyber appendix. City Cybersecurity team will facilitate and support exercise preparation.

When you protect your Department, you protect the whole City. Thank you for supporting our collective cyber defense and protecting the City against costly cyberattacks.

Table of Contents

Table of Figures

Figure 1- ESF 18 Unified Cyber Command Flow Chart

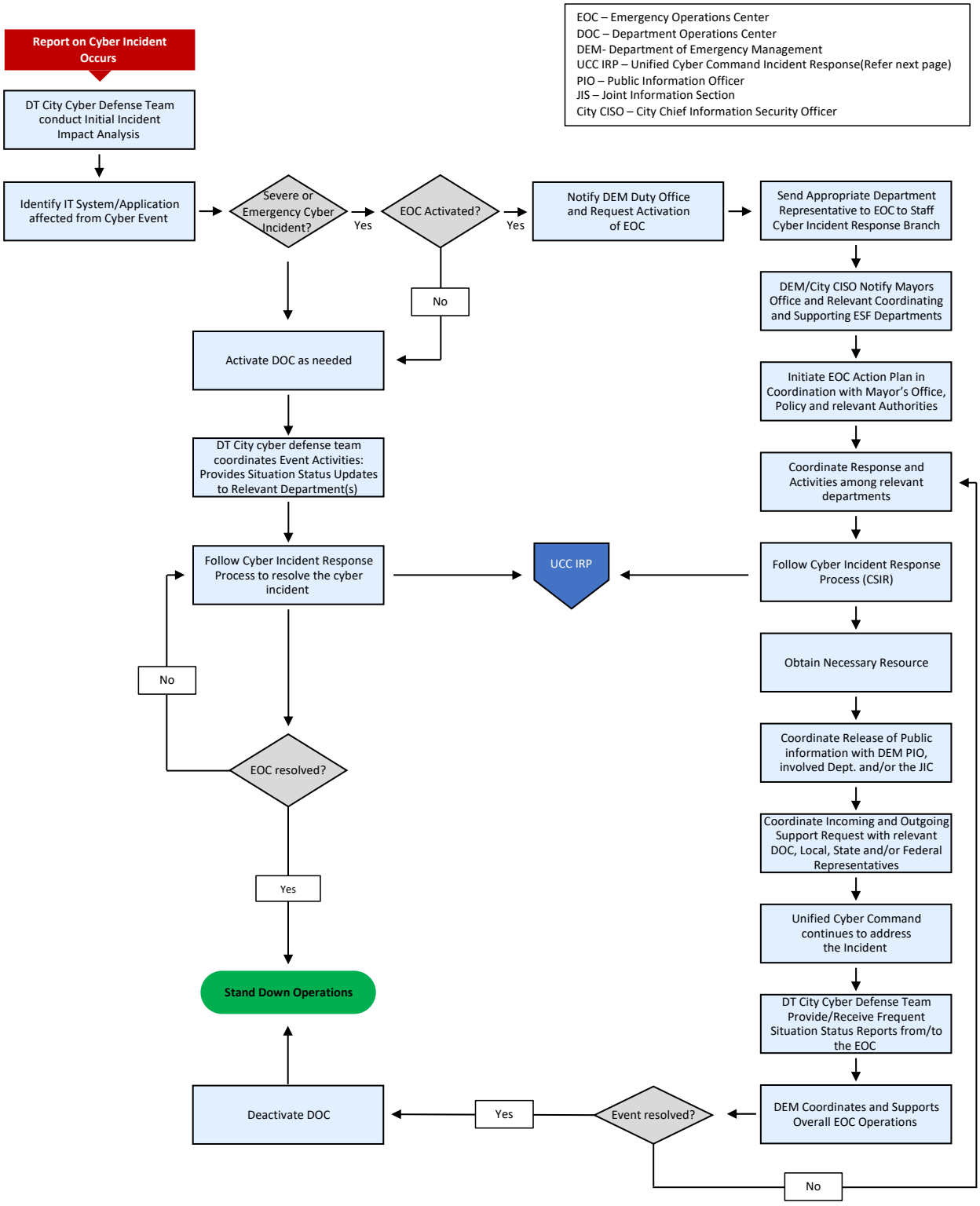
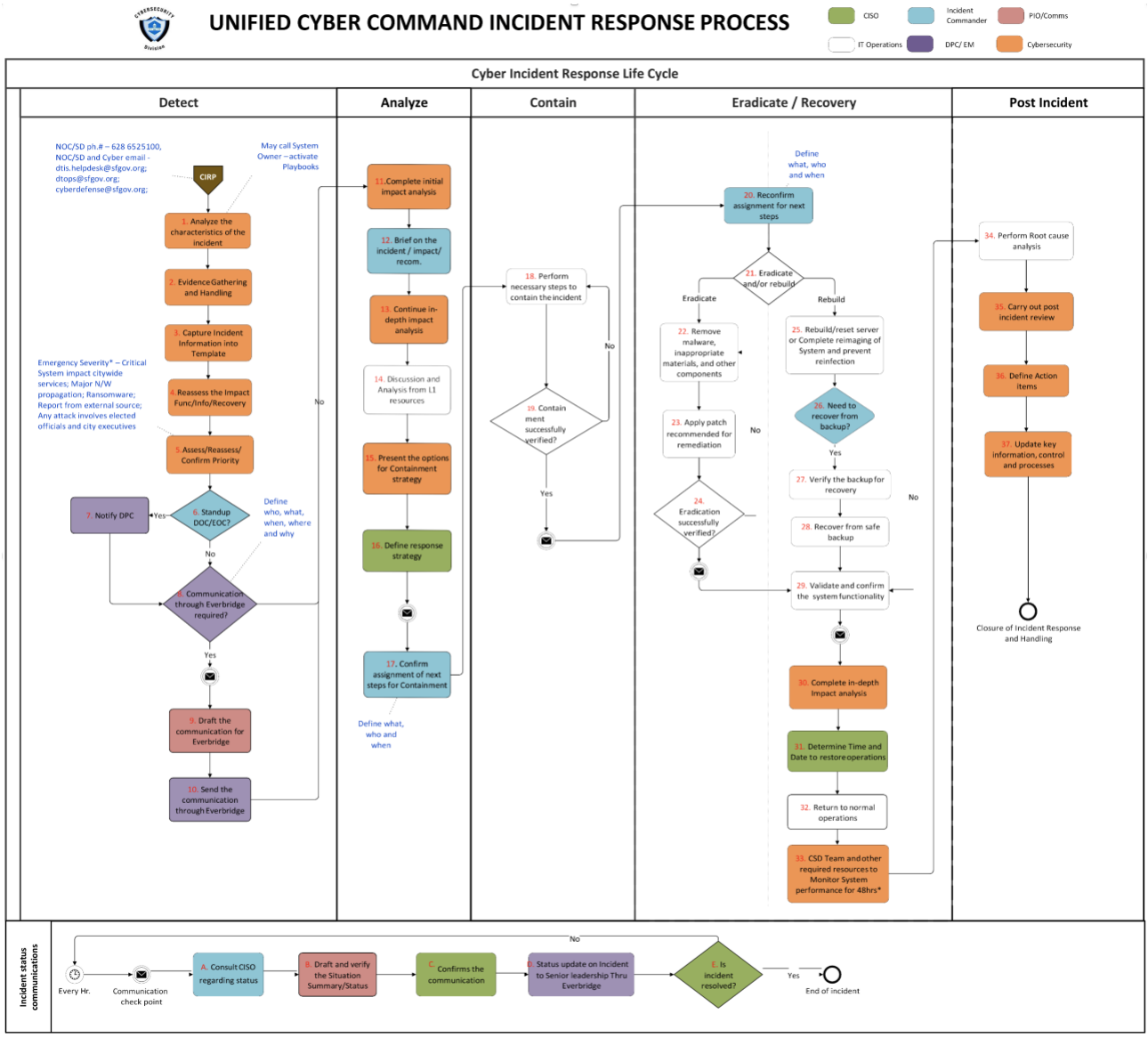


Figure 2- Unified Cyber Command Incident Response Process



Section 1: Introduction

1.1 Coordinating and Supporting Departments

Coordinating Department	Department of Technology (DT) - City Cyber Defense Team
Primary Supporting Department(s)	DT - Network Operations Center (NOC), DT - Infrastructure and Operations Team (I&O), Department of Emergency Management, Controller's Office, San Francisco Police Department, City Administrator, City Attorney, Department of Human Resources, City Chief Auditor and Risk Management, Office of City Administrator
Secondary Supporting Department(s)	All City Agencies
Critical Supporting Partners	Norther California Regional Intelligence Center (NCRIC), State and Federal Agencies with cybersecurity capabilities, and CCSF Contracted cybersecurity vendor resources

1.2 Departments and Partners Responsibilities

Department	High-level Responsibilities
City Cyber Defense Team	• Coordinate CCSF ESF #18 activities • Maintain contact with Departmental Information Security Officers and/or DOC(s) involved with responseoperations • Staff EOC Cybersecurity Branch as required • Coordinate the use of additional cybersecurity resources • Provide ongoing situation status updates • Maintain communication with City Leadership and Departments • Request Mutual Aid when needed
Primary and Secondary departments	• Report cybersecurity incidents to the City Cyber Defense team by calling the 24/7/365 Network Operation Center at **628-652-5100** • Send a representative to the relevant DOC(s) or EOC to assistwith cybersecurity activities • Provide ongoing status updates to the EOC and/or DOC • Support cyber incident response and recovery process • Perform other emergency responsibilities as assigned
Critical Supporting Partners	• Facilitate the exchange of law enforcement-sensitive threat intelligence information with State and Federal resources tosupport Cyber incident response. • Collect and disseminate threat intelligence andinvestigative information • Provide contracted cybersecurity services, including cyber sensor monitoring, threat detection, incident investigation, incident response, forensics, and crisis management

1.3 Purpose

The purpose of this *Emergency Support Function (ESF) #18: Unified Cyber Command Annex* is the following:

- establish a unified understanding of key cyber concepts andterminologies
- provide a system to evaluate the severity of a cyberincident
- assign roles and responsibilities to City stakeholders

The plan is specifically focused on priority SEVERE or EMERGENCY cyber incidents, when the City's Emergency Operations Center (EOC) is activated to coordinate:

- key processes for sharing threat intelligence
- develops situational awareness
- manages operational response in a cyber- disrupted environment

1.4 Scope

ESF #18: Unified Cyber Command Annex plan addresses cyber incidents that have or could potentially degrade, damage, or destroy information systems in City Departments, Agencies, Offices, and Commissions. High focus will be given to cyber incidents affecting City government critical functions and infrastructure, including:

- Medical/Healthcare Services
- Government/Public Safety Services
- Financial/Banking Services
- Transportation/Transit Services
- City's Telecommunications Services
- City's managed Lifelines - Critical Infrastructure
- City's Radio Infrastructure
- City and Department IT Networks
- City and Department Enterprise Technology and Applications

This plan focuses on mitigating and responding to the consequences created by the incident. This plan does not address ongoing cybersecurity measures or pre-incident system vulnerability assessments.

City Departments will utilize this plan as the basis for development and maintenance of subordinate plans, response policies, and implementing procedures, such as Cyber Annex Plans to their IT Continuity of Operations Plans (IT COOPs).

Cybersecurity incidents are required to be reported to the City Cyber Defense team by calling the City 24/7/365 Network Operation Center (NOC) at **628-652-5100**. The City Cyber Defense team will prioritize the incidents using the priority matrix on the following page. If an incident is assessed to be Priority SEVERE and EMERGENCY, then the incident is determined to be a Major Incident.

1.5 Authorization and Compliance

This plan was developed to comply with the COIT Citywide Cybersecurity policy https://sfcoit.org/cybersecurity . The COIT Cybersecurity Policy requires all departments to: Support cyber incident response as needed in accordance with Emergency Support Function 18 (ESF-18) Unified Cyber Command.

1.6 Unified Cyber Command Priority Matrix

The following schema is a method for rating the current or potential priority of a cyber incident in CCSF Departments.

Cyber Incident handled by			Criteria (only one criteria match is needed to define priority level)
GUARDED	Department Incident Management	For departments monitored by Unified Cyber Command, City Cyber Defense team will guide with analysis, containment, response, forensics and recovery phase of cyber incident. **Note: Severe and Emergency Incidents – City leadership to be notified**	1. Initial report of a cyber event. 2. Unlikely to impact public health or safety, or city services. 3. Likelihood that level 3-5 data* (i.e., Sensitive, Protected or Restricted) has been exposed internally only 4. Malware or malicious content that has a low probability of spreading, such as malware detected by an anti-virus on a workstation
IMPORTANT	Department Incident Management		1. Compromise of non-critical Department's systems as identified in the Department's IT COOP 2. Malware discovered on servers and Infrastructure supporting non- critical Department's systems as identified in the Department's IT COOP 3. Likelihood that level 3-5 data has been exposed to a limited external group, such as unauthorized external partners * **Data Classification:** https://sfcoit.org/sites/default/files/201909/DataClassificationStandard_FINAL_DRA FT.pdf
SEVERE	DOC Activation		1. Compromise of Department's systems with Medium impact to its mission as identified in the Department's IT COOP 2. Compromise of Citywide systems, public facing systems or major City supplier systems 3. Malware spreading to Department systems (multiple infections in a short period of time affecting Department users). 4. Likelihood that level 3-5 data is widely exposed externally –(Significant number of record)
EMERGENCY	EOC & DOC Activation		1. Poses a threat to the provision of wide-scale critical infrastructure services, City government security, or the lives of City residents. 2. Compromise of Department's systems with High impact to its mission as identified in the Department's IT COOP 3. Compromise or loss of availability of systems responsible for City's critical functions and infrastructure (section 1.4)* 4. Malware affecting multiple Departments or spreading at a rapid rate on the network

Section 2: Concept of Operations

2.1 General Concepts

As the threat of or an actual cyber incident develops, the City Cyber Defense Team will lead the initial cyber response. The City Cyber Defense Team will communicate with Departmental Information Security Officers (DISOs) and other designated IT staff in affected agencies as well as state and federal resources to identify the threat, develop threat intelligence, and analyze actual or potentially affected systems, and work to remediate the incident.

The City Cyber Defense Team will notify and coordinate with DEM for Priority SEVERE and EMERGENCY cybersecurity incidents. If warranted, DEM will activate elements of the City's Emergency Response Plan (ERP). This could result in the activation of the EOC to facilitate information sharing, resource development, and operational coordination.

The ESF #18 Concept of Operations outlines

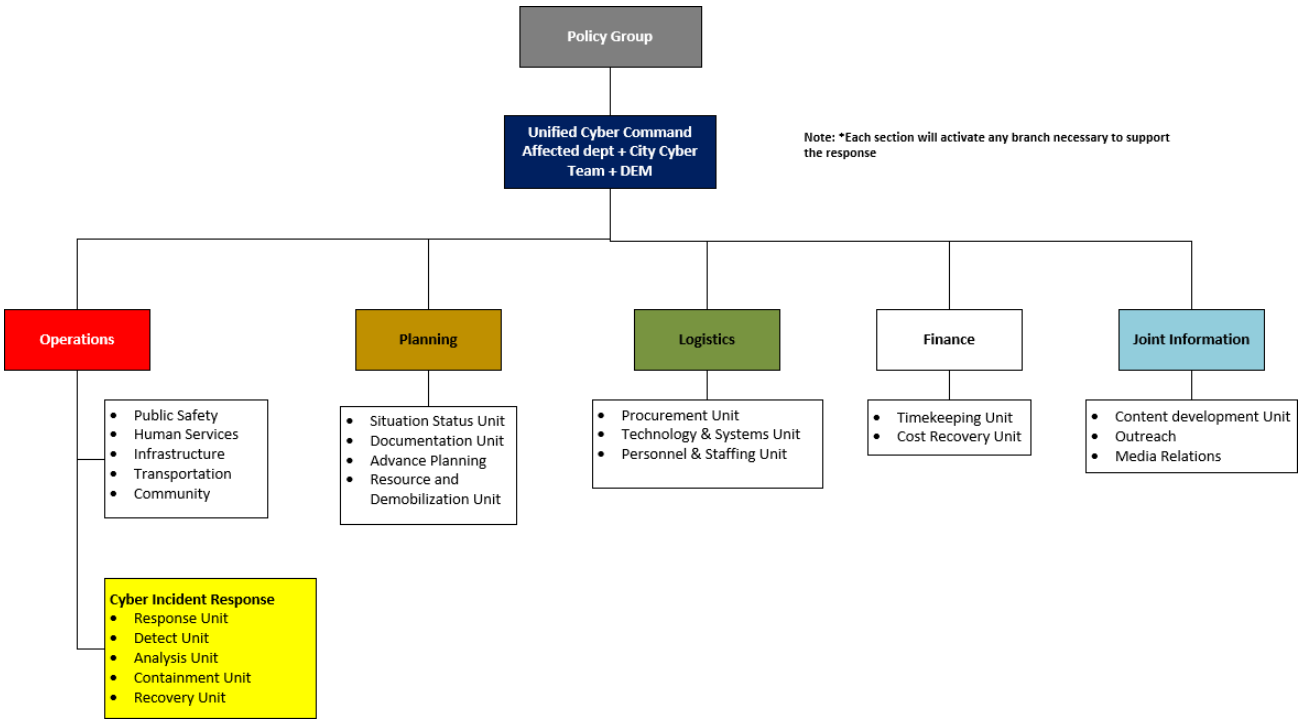
1. Unified Cyber Command Structure
2. Unified Cyber Command Key Response Activities
3. Unified Incident Response Process

2.2 Unified Cyber Command EOC Structure

CCSF has organized the ESFs in accordance with ICS to comply with the National Incident Management System (NIMS). During an ESF #18 EOC activation, each section in ICS will be headed by a CCSF representative carrying out the role as defined in the figure below depicts the standard ESF #18 ICS organizational structure.

For large emergencies, the EOC may serve as the central location for interagency support and coordination, including activities associated with ESF #18.

Figure 3- Unified Cyber Command EOC Structure



2.3 Unified Cyber Command Key Response Activities

Key Cyber Incident Response Activities			
	Department-led activities	**City Cyber Defense Team-led activities**	**DEM-led Activities**
PRIORITY: SEVERE	**1. If Department discovers the cyber incident, Reports immediately to the City Cyber Defense team(628-652- 5100)** **2.** Department activates its Department Operations Center (DOC) **3.** Departmental Information Security Officer uses Department Cyber Annex procedures to lead the incident analysis and remediation activities. Forensic evidence may need to be preserved for future criminal investigation or prosecution. **4.** The Departmental Information Security Officer provides regular updates to the City Cyber Defense team **5.** Departmental Compliance Personnel and City Attorney need to be notified for data exposure incidents **6.** Department Head approves return to normal operations upon consultation with the Department Information Security Officer and the City CISO	1. **If City Cyber Defense team discovers the incident - notifies the affected Department Information Security Officers, City Chief Information Security Officer (City CISO) and City Chief Information** Officer (City CIO) 2. Notifies DEM for situational awareness and if required confirms EOC activation 3. Supports requests from affected Department DOC and provides assistance for its cyber incident response 4. Activates DT DOC; if affected systems are managed and supported by DT 5. Works with the Critical Supporting Partners to monitor the incident and conduct Citywide network and system analysis 6. Supports forensic certification required to validate eradiation of malware prior to return of business applications to production service	1. City Emergency Operations Center (EOC) activation may be desirable 2. If EOC is activation is required, follow DEM led activities 3. Affected Department PIO is notified and activates citywide joint information systemin coordination with the DEM PIO and the Mayor's PIO to provide San Franciscans consistent messaging
PRIORITY: EMERGENCY	**1. If Department discovers the cyber incident, Reports immediately to the City Cyber Defense team (628-652- 5100) for EOC activations** 2. Department activate its DOC and supports all activities at EOC 3. Departmental Information Security Officer uses Department Cyber Annex procedures to support the incident analysis and remediation activities (Note: Affected Departments with stand-alone networks, data centers, or email will need to take primary role in incident analysis and remediation. Unified Cyber Command will review and assist with incident response plan prior to any remediation action to ensure Citywide impact is known and City leaders and key supporting partners are consulted) 4. Departmental Compliance Personnel are notified and assist with incident	**1. If City Cyber Defense team discovers the incident - notifies the affected Department Information Security Officers, City Chief Information Security Officer (City CISO) and City Chief Information Officer (City CIO)** **2.** Notifies DEM for EOC activation **3.** Leads and supports all EOC activities with affected Department Information Security Officers **4.** Notifies Critical Supporting Partners, including incident response vendors, state and federal agencies with cybersecurity responsibilities **5.** Supports citywide collection of forensic evidence for future criminal investigation and prosecution **6.** Based on the analysis, information provided by the Departmental Information Security Officers and Critical Supporting Partners, the City Cyber Defense team formulates and executes a cyber incident response plan **7.** Supports forensic certification required to validate eradiation of malware prior to return of business applications to production service	1. EOC is activated 2. DEM coordinates the City's ESF 18 - Unified Cyber Command Process 3. Notification to policy group, City leaders and City Attorney 4. Consults with Policy group about the impacts to cyber incident 5. Coordinates with Unified Cyber Command for regular status and situational updates to City leaders 6. The Joint information section disseminates consistent messaging about the incident 7. Policy Group approves return to normal operations upon consultation with the City CISO and City CIO

2.4 Unified Cyber Command Incident Response Process

The following section will describe Unified Cyber Command Incident Response Phases, key response activities, roles and responsibilities and information necessary to respond to a cyber incident.

Phase	Objective
1. Preparation	Identify activity or work that should be completed to make the response successful
2. Reporting and Detection	Provide channel to report suspected incidents and verify that an incident has occurred
3. Analysis, Notification and Escalation	Understand the incident and begin notifications and escalations
4. Containment	Stop the incident from spreading further and eliminate further damage
5. Eradication	Determine the root cause and fully eliminate it as well as the symptoms everywhere
6. Recovery	Return to normal operations
7. Post Incident Review	Close out the incident and determine areas for improvement

The preparation phase is an ongoing phase focused on preparing the organization and the response team for preventing and handling security incidents. An active process, where a specific security incident is being worked towards resolution, consists of phases 2-6 and continues through those phases until a resolution is reached. The last phase, post incident review, is an opportunity to look back at the activities and outcomes for a specific security incident and find opportunities for continuous improvement. Each phase has a different set of activities that are undertaken to ensure the successful resolution of security incidents.

2.4.1 Preparation

Preparedness is a continuous cycle of planning, organizing, training, equipping, exercising, evaluating, and taking corrective action across mission areas (i.e., prevention and protection) to ensure effective coordination during cyber incident response.

The Coordinating Department is responsible for overseeing the implementation of preparedness activities. Goal is to prepare the team/ establish the procedures/ plans/ elements needed for incident handling to take place.

2.4.1.1 Roles and Responsibilities

Role	Responsibilities
City CISO	• Facilitates the ESF 18 Unified Cyber Command annex document and ensure it is reviewed annually and updated as needed • Ensures that key stakeholders are familiar with and trainedin the cybersecurity incident response process • Facilitates annually cybersecurity tabletop exercises and discussion with DISOs • Leads annual review of Cyber incident response procedure • Ensures that contracts are budgeted and in place for outside vendors that could be engaged as a part of an active cybersecurity incident
Departmental Information Security Officers	• Actively participate in CIRP activities in all phases • Participate in annual review of CIRP documentation • Participate in annually cybersecurity tabletop exercises and discussion
JIC Cyber Communications	• Work with the City Cyber Defense Team to maintain a list of communication templates for different types of incidents and seek ongoing input from the JIC, Department PIO and City Chief Information Security officer so that communications are timely in the event of a cybersecurity incident
IT Department and Line of Business Staff	• Attend trainings and understand individual and work unit responsibilities in the event of a cybersecurity incident • Participate in annually cybersecurity tabletop exercises and discussion as requested by their DISO • Provide adequate support during business hours and, if applicable, after hours
Disaster Preparedness Coordinator (DPC)/ Emergency Manager (EM)	• Annually review COOP for essential services and their interdependencies and cyber annex consider any edits to the currentsituation • Train department leadership and cybersecurity incident response staff with Department and Emergency Operation Center roles and responsibilities • Participate in annually cybersecurity tabletop exercises discussion and trainings as requested by • CIRP core team members

2.4.2 Reporting and Detection

Reporting incidents is the responsibility of all CCSF staff, city agencies and security partners. Suspected cybersecurity incidents should be reported to the City Cyber Defense team by calling the City 24/7/365 Network Operation Center (NOC) at 628-652-5100.

Detecting a cybersecurity incident can occur in a variety of forms. Primary detection mechanisms are alarms from cybersecurity protection measures or reports from CCSF agency, staff and security partner. In this phase affected CCSF agency or staff and security partner are responsible to notify the City Cyber Defense Team. Events that may reasonably be considered adverse should be reported, initiating the incident response process. Such events may be detected through several mechanisms, including by the City cyber defense team ongoing monitoring operations, by divisional or local IT and security teams or by end users. The City cyber defense team will discover the majority of potential incidents through security monitoring.

The goal of this phase is twofold:

1. Identify and categorize potentially adverse events
2. Ensure that the appropriate individuals are promptly informed of these events, placing them in a position to take action

2.4.2.1 Roles and Responsibilities

Role	Responsibilities
Department – DISO, IT Support Staff and DPC/EM	• Report cyber incident by calling the City 24/7/365 Network Operation Center (NOC) at **628-652- 5100** • Department may activate its DOC • Use Department Cyber Annex procedures to support incident during detection • Coordinate with City Cyber Defense team with necessary information to validate and detect the cyber incident
DT NOC	• Take initial incident report • Recognize the incident is a cybersecurity incident • Notify the on-call City Cyber Defense Team analyst • Act as Major Incident Commander until incident is handedoff to On-call City Cyber Defense Team
On-call City Cyber Defense Team Analyst	• Engage subject matter experts as needed to quickly validate cybersecurity incident • Notify Cyber Defense Manager • Notify City CISO

2.4.3 Analysis, Notification and Escalation

During the analysis phase, the affected City Department coordinates with the City Cyber Defense team, which involves recording available reporting observations, assessing potential incident severity, and determining the type of incident that has occurred. In general, this phase requires the City Cyber Defense team to review playbooks, collect, analyze information and determine next steps.

This phase has the following goals:

- If necessary, confirm the validity of information provided in the initial lead
- Determine whether the event is a cause for concern or a false positive
- Determine whether further investigation is warranted
- Determine priority of the incident
- Determine need to activate City's Emergency Operation Center
- Determine immediate Remediation steps

Cyber incidents may be difficult to identify and their impacts not immediately apparent. As a cyber incident develops, timely and flexible coordination is needed to alert and notify key stakeholders. Based on the information provided, additional stakeholders will be identified, and the DEM Director will determine whether the EOC will be activated to a Level II (Partial). If there isn't a change in the EOC activation level, the City Cyber Defense Team and DEM will establish a timeframe for further briefings.

2.4.3.1 Roles and Responsibilities

Role	Responsibilities
City Cyber Defense Team	• Receive initial reports • Complete Master Response Process • Review Threshold Indicators • Declare active cybersecurity incident to engage and activate resources • Identify incident priority • Gather additional information and engage key players for further analysis • Determine if escalations are needed and work with the City Cyber Defense Team Manager to make those decisions (ongoing) • Participate in Information Gathering call (if needed) • Contact partners (if needed) • Participate in Situational Awareness conference call: • Provide updated information
Departmental Information Security Officer (DISO) of the Affected Department	• Support in incident response process by providing Departmental logs, alerts, network and application diagrams, and installing required City cybersecurity tools for investigation and forensics
DEM EOC Incident	• Initiate conference bridge as needed (ongoing), if after hours, send notifications to key stakeholders (ongoing)

Commander	• Notify DEM / Division Directors • Contact partners and stakeholders (if needed) • Coordinate/lead Situational Awareness conference call: • Review Information Requirements • Determine EOC Activation Level • Send status updates/ situation summary at regular intervals as well as when the incident moves from one phase to another • Determine additional recipients that need to be included in ongoing updates (e.g. initial end user, site owners, server owners)
City Attorney	• Establish attorney–client privilege • Provide guidance on preserving evidence • Analyze City regulatory compliance obligations
City Administrator	• Provide as needed guidance for incident response plan
City CISO	• Notify City Cybersecurity Advisory Team (City Administrator, City Controller, City Attorney, City CIO, City Auditor, DEM, DHR, Risk Management) • Provide City leadership and policy group with directions on escalation and decisions • Determine the Incident Priority • Determine response plan
Controller's Office	• Establish incident and project codes for cost recovery purposes • Oversees the coordination of all financial policy, employee compensation, accounts payable, and cost recovery related to the incident
Policy Group	• Advise and assist the Mayor on policy issues affecting CCSF and Respond to requests for policy direction from the EOC
City Risk Manager	• Notify and brief City cyber insurer • Work with Controllers office and Cyber insurer to track recovery cost
PIO	• Serves as the point of contact for the JIC, which coordinates and disseminates event information to the public, the media, and other relevant stakeholders.
Disaster Preparedness Coordinator (DPC)/ Emergency Manager (EM)	**During an active incident:** • Assess if a DOC activation is needed to support any departmental logistical needs for both during work hours and after hours • Maintain situational awareness of incident and its current and long-term impacts to any business operations. • Coordinate any messaging with department heads/senior staff and PIO/JIC group • Participate in any IMT Conference calls

2.4.4 Remediation: Containment, Eradication and Recovery

The Remediation phase encompasses containment, eradication, and recovery activities.The goals of remediation are to remove the threat from the system environment and restore systems to normal operational condition. Remediation planning should begin immediately upon determining an incident has occurred.

Containment - The goal of containment is to limit damage from the current security incident and prevent any further damage.

Eradication - Eradicating the threat from a compromised system often means rebuilding that system using a trusted image. Though it may be possible to remove many types of malware from a system without rebuilding it, the affected system/application must be forensically certified before it is connected to the production environment. Eradication may also depend on requirement from law enforcement is a cyber incident becomes part of an active investigation.

Recovery - Recovering from a cyber incident requires close coordination across all affected Departments and teams within a Department and may include the need to consider legal implication if sensitive data is breached. Depending on the nature and scope of the cyber incident, a criminal investigation and evidence activities may continue well beyond activation of this plan.

2.4.4.1 Roles and Responsibilities

Role	Responsibilities

City Cyber Defense Team	• Draft Remediation Strategy
	• Verify Containment and/or Eradication activities
	• Identify security weaknesses required to be addressed prior to full recovery of affected systems
	• Initiate and complete in-depth detailed analysis
	• Preserve and store data while ensuring chain of custody for investigations after containment (ongoing)
	  ○ Investigate potential loss of data (ongoing)
	  ○ Coordinate with security partners and State and Federal agencies
	  ○ Provide regular status updates to DEM EOC Commander

Departmental Information Security Officer	• Contribute to the Remediation Strategy • Assist with affected system containment • Assist with eradicating malware • Supports recovery and/or rebuild of affected systems and closure of identified weaknesses (such as patching vulnerabilities or changing passwords) • Supports forensics on restored systems to verify their production readiness

Department of Technology	• Assist with drafting of Remediation Strategy
	• Implement Remediation Strategy, including
	  ○ Contain affected system
	  ○ Remove malware
	  ○ Recover and/or rebuild affected systems and closure of identified weaknesses (such as patching vulnerabilities or changing passwords)
	• Support forensics on restored systems to verify their production readiness
	• Provide regular status updates to DEM EOC Commander

City Attorney	• Determine legal risk management plan • Prepare breach notification
City CISO	• Provide leadership and direction on escalation decisions as needed (ongoing) • Determine Remediation Strategy • Confirm in-depth impact analysis completion • Certify that systems/applications are approved to be re- connected and be put into productions • Approve the return to normal operations.
Risk Management	• Prepare required documentation for insurance submission and cost recovery
Policy Group	• Review and advise on the Remediation Strategy • Support activities required for return of normal operations, including allocating IT and Business staff to remediation activities

DEM EOC Commander	• Continue conference bridge (ongoing)
	• Coordinate/lead Situational Awareness conference call:
	  ○ Review Remediation Strategy
	  ○ Review current remediation status
	• Send status updates/ situation summary at regular intervals as well as when the incident moves from one phase to another

PIO	• Serves as the point of contact for the JIS, which coordinates • and disseminates event information to the public, the media, and other relevant stakeholders.
Department Finance and Procurement Team	• Supports Emergency procurement, employee compensation, accounts payable, cost recovery and insurance claims.

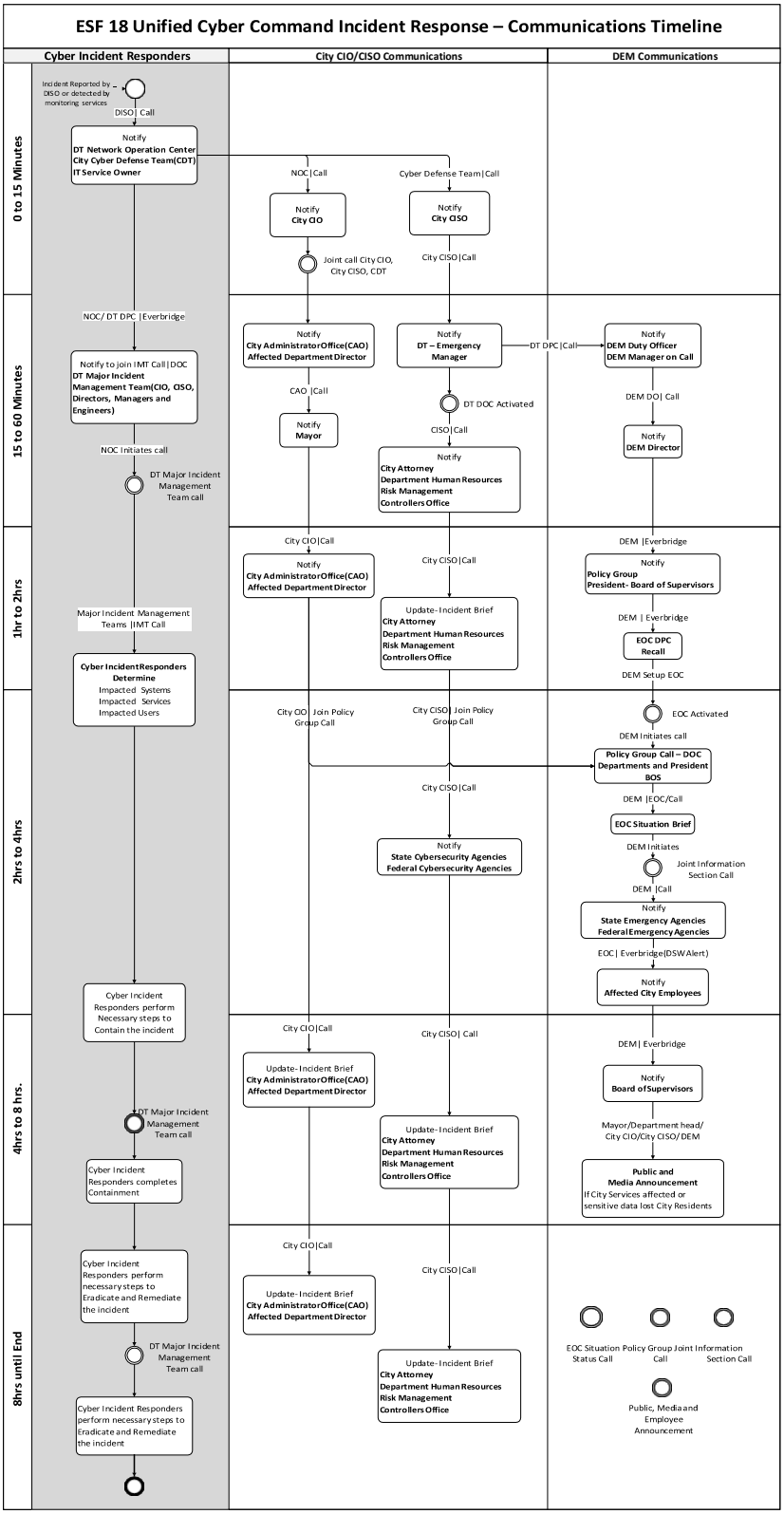
2.4.5 Post Incident Review

The objective of the post-remediation phase is to revisit the root cause and outcome of each security incident to identify activities, controls, or policies that will help prevent future incidents. An After-Action Report is required for all major incidents. While responding to incidents, responders should document the actions they executed, and the evidence observed. For routine incidents, much of this information will be documented in the ticketing system and incident report. More complex or impactful incidents should be documented in a formal After-Action Report.

2.4.5.1 Roles and Responsibilities

Roles	Responsibilities
Department of Emergency Management	• After resolution of cybersecurity incident, coordinate and facilitate a post incident review • Circulate the incident report for feedback as needed • Communicate the results of the post incident review via incidentreport
City Cyber Defense Team Manager	• Follow through on action items from the post incident review as they relate to continuous improvement of the cybersecurity incident process • Make updates to CIRP documentation as needed
City CISO and Departmental Information Security Officers	• Participate in post incident review and provide input
City Cyber Advisory Team	• Participate in post incident review and provide input

Appendix 1: Communication Timeline for SEVERE and EMERGENCY



Appendix 2: Cyber Incident Response Checklist

#	Tasks	Responsibility
☐	Report a cyber incident (or suspicion of an incident) to City Cybersecurity Team **24/7/365 at 628-652-5100**	**Affected Department/ City Cybersecurity Team**
☐	Do not restart or turn off systems – this can destroy evidence and alert attackers. Work with City Cybersecurity team to investigate	
☐	Classify incident priority using ESF-18 priority matrix and kick off incident response below	
For Emergency or Severe or Important		
☐	Initiate ESF18 Communication Protocol	**City CIO and City CISO**
☐	Brief Cybersecurity Advisory team (City Administrator, City Controller, City Attorney, City CIO, City Auditor, DEM, DHR, Risk Management)	**City CISO**
☐	Notify law enforcement	
☐	Form Cyber Incident Response team	**City CISO, Affected Department, City Cybersecurity Team, City IT teams**
☐	Determine if an active attack is underway by analyzing affected systems and credentials. Work with vendors for vendor breach.	**Cyber Incident Response team**
☐	Isolate breached systems and reset/disable credentials	
☐	Remove malware and fix breached systems. Remediation must allow preservation of attack evidence for law enforcement needs.	
☐	Brief City cyber insurer	**City Risk Manager/ City CISO/ City Attorney**
☐	Joint Information Section (JIC) – Create communications plan to public, media relations and affected agencies/people	**Joint Information Section (JIC) Affected department/DEM/ City Administrator/ DT/ Mayor's office**
☐	Restore services post incident. Services must not be restored until remediation is complete and validated.	**Affected Department/ City Cybersecurity Team**
☐	Perform complete root cause analysis	

Appendix 3: Data Breach Response Checklist

#	Tasks	Responsibility
☐	If a breach is suspected, contact City Cyber Team **24/7/365 at 628-652-5100**	**Affected Department/ City Cybersecurity Team**
☐	Validate the data breach (review access, system and network logs). Identify the type of data breached.	
☐	Classify breach priority: **Emergency** or **Severe** or **Important** (see definitions below)	**Affected Department/ City Attorney/City CISO**
☐	Initiate ESF18 Communication Protocol	**City CIO and City CISO**
☐	Initial briefing with Policy Group and Cybersecurity Advisory team	**City CIO, City CISO, City Attorney**
☐	Incident response management team defined mitigation plan	**Affected Department/ City CISO/ City Attorney**
☐	Work with City Risk Manager to notify City cyber insurance	**City Risk Manager/ City CISO/ City Attorney**
☐	Work with City Controller to establish a data breach incident and project codes for cost recovery purposes	**Affected Department**
☐	Follow-up briefing with Policy Group and Cybersecurity Advisory team	**City CIO, City CISO, City Attorney**
☐	Joint Information Section (JIC) – To draft, review and finalize communications plan to public, media relations and affected agencies/people Create a web page that is clearly accessible from the home page of affected department home page site that is written in plain English	**Affected department/DEM/ City Administrator/ DT/ Mayor's office**
☐	Early communication to the City family in the soonest time possible	**Affected department/JIC**
☐	Early communication to the affected people in the soonest time possible – inform affected people and follow up with detail later.	**Affected department/JIC**
☐	Build and staff call center/ hotline to handle communications to affected people	**Affected Department**
☐	Contact affected people about the breach by all known methods (message about breach and credit monitoring service)	**Affected department/JIC/City Attorney**
	If there is action for users to take, communicate it clearly – print out instructions and send them with the official notice by mail, and have them easy to access on the homepage of their website.	**Affected department/JIC**

Cyber Incident handled by			Criteria (only one criteria match is needed to define priority level)
GUARDED	Department Incident Management	For departments monitored by Unified Cyber Command, City Cyber Defense team will guide with analysis, containment, response, forensics and recovery phase of cyber incident. **Note: Severe and Emergency Incidents – City leadership to be notified**	5. Initial report of a cyber event. 6. Unlikely to impact public health or safety, or city services. 7. Likelihood that level 3-5 data* (i.e., Sensitive, Protected or Restricted) has been exposed internally only 8. Malware or malicious content that has a low probability of spreading, such as malware detected by an anti-virus on a workstation
IMPORTANT	Department Incident Management		4. Compromise of non-critical Department's systems as identified in the Department's IT COOP 5. Malware discovered on servers and Infrastructure supporting non- critical Department's systems as identified in the Department's IT COOP 6. Likelihood that level 3-5 data has been exposed to a limited external group, such as unauthorized external partners * **Data Classification:** https://sfcoit.org/sites/default/files/201909/DataClassificationStandard_FINAL_DRA FT.pdf
SEVERE	DOC Activation		5. Compromise of Department's systems with Medium impact to its mission as identified in the Department's IT COOP 6. Compromise of Citywide systems, public facing systems or major City supplier systems 7. Malware spreading to Department systems (multiple infections in a short period of time affecting Department users). 8. Likelihood that level 3-5 data is widely exposed externally –(Significant number of record)
EMERGENCY	EOC & DOC Activation		5. Poses a threat to the provision of wide-scale critical infrastructure services, City government security, or the lives of City residents. 6. Compromise of Department's systems with High impact to its mission as identified in the Department's IT COOP 7. Compromise or loss of availability of systems responsible for City's critical functions and infrastructure (section 1.4)* 8. Malware affecting multiple Departments or spreading at a rapid rate on the network

Appendix 4: Template – Department Name COOP Cybersecurity Appendix

***Department Name*- Continuity of Operations Plan**

***Department Name*-** Cybersecurity Appendix

The purpose of this appendix is to link your department continuity of operations plan (COOP) to the city Unified Cyber Command Plan (ESF-18). Your COOP describes the steps department personnel will take if there is a disruption in normal operations. The cybersecurity annex identifies the steps department information technology staff will take if the disruption is cyber-related. It also describes how the information technology team will work with the department preparedness coordinator to jointly respond to the incident, continue department operations, reconstitute essential systems and return to normal operations.

Begin by identifying the essential functions your department/division is responsible for. This information can be found in your continuity of operations plan essential functions worksheet

Essential Function		Supporting IT Systems
1		
2		
3		

An event has three phases: before (pre), response (during) and recovery (after). Answer the following questions to document the resources available, individuals that need to be notified and steps the IT team and DPC will take relating to a cyber event.

Pre event	Department Response
1. What are the tools and techniques used to analyze system health?	*List of Tools:* *List techniques:* *Which group/team is involved in performing analysis in your department?*
2. How will you ensure that your Department IT and operational staff are available to support cyber incident response and recovery process?	*Who in your department will own this responsibility?*
During an event	**Department Response**
3. What are the tools and techniques used to analyze a cyber incident?	*List of Tools:* *List techniques:* *Which group/team is involved in performing analysis in your department?*
4. How and when will the Department Information Security Officer (DISO) get notified of an incident?	*Who will notify DISO?* *Do you have your DISO contact information stored?*
5. Who will evaluate the impact of the incident to the Department business operations?	*DPC? DISO? Any other group?*
6. How would this issue be reported in your Department IT leadership?	*Email? Phone Call? Everbridge?*
7. Classify your department critical IT applications/systems based on ESF priority Matrix	*Collect this information from your IT Team and Add this information on COOP*
8. What priority will be assigned based on ESF 18 Matrix?	*How and who will determine the priority*
9. How and who will notify the City Cyber defense team?	*Collect this information from your DISO*
10. What is the process and who will be involved to manage emergency response?	*Who owns the process? Is training provided to your dept IT/ cybersecurity staff on emergency response process?*
11. Do you have sufficient Department IT staff to support remediation and rebuilding at the same time for dozens/hundreds of users?	*Who is responsible to gather collect this information? How is this information collected*
12. How are communications handled internally to department staff and senior management?	*Phone? Email? Everbridge? Social Media?*
13. What's the department guidelines on media relations?	*Collect this information from your department PIO or Communications Team*

14. Who is designated to talk to the press?	*Collect this information from your department PIO or Communications Team*
After an event	**Department Response**
15. Who in the Department will request and approve emergency procurement for laptops or server equipment?	*Collect this information from your Department Finance*
16. As restoration may take several months, have you determined alternate/back up procedures to continue your Department operations without internet and computers in your Department COOP?	*Collect this information from your Department Management and IT Teams*
17. How are you tracking costs of getting your system back online?	*Collect this information from your Department Finance*

Appendix 5: Sample Cyber Incident Action Plan

Note: If a formal Incident Report is necessary, this template provides an example format for that. In many cases, information documented in the ticketing system may meet reporting requirements.

Hostname (affected system or device)	**IP Address**	**Operating System**
HOSTNAME	xx.xx.xx.xx	OS TYPE
Network	**System Owner**	**Host Type**
Network	USERNAME	[DESKTOP/SERVER/LAPTOP]
Date	MM/DD/YYYY	
Identification Time	HH/MM [AM/PM] [TZ]	
Physical Location	[Location] City, State	
Description		
Source of Notification: Examples: ▪ End user or IT help desk ▪ Email from customer ▪ SIEM alert *Stakeholders outside the Operations function:* Examples: Business representatives like Program Managers, groups such as Human Resources. *Obligations to disclose data loss that may be applicable:* Examples: Contractual obligations to customers, regulatory compliance, etc. *Incident Summary:* A brief explanation of the incident describing what the initial lead was, the threat classification, any tasks assigned and to whom they were assigned, and a general description of the plan to investigate		
Business Impact		

Incident Severity Rating	

Type of Incident (select one)							
☐	Common Malware	☐	Phishing Attempt	☐	Compromised Public Host	☐	Backdoor
☐	Advanced Threat	☐	Violation of acceptable use	☐	Unauthorized network activity	☐	Unauthorized Software
☐	Denial of Service	☐	Controlled data spill	☐	Lost/Stolen Laptop	☐	Other

If other, explain	There may be situations when the process of investigation is required to determine the type of incident. This field should be used to provide a description of those events.
Forensic image hash (if acquired)	

Supporting Details
Use this space to describe, in detail, the investigation

Conclusions and Recommendations
Use this space to describe any conclusions and lessons learned

Appendix 6: Unified Cyber Command Communications Plan

Emergency Support Function #18, which details the City's operational response in the event of a cybersecurity incident, is available for view on the DEM website, along with the City's wider Emergency Response Plan. In the event of an incident, the Department of Emergency Management, the Department of Technology, the Mayor's Office, and any affected other departments will respond according to ESF 18. This plan is intended for use during an emergency-level incident, as defined by the ESF:

SEVERE	• Compromise of Department's systems with Medium impact to its mission as identified in the Department's IT COOP • Compromise of Citywide systems, public facing systems or major City supplier systems • Malware spreading to Department systems (multiple infections in a short period of time affecting Department users). • Likelihood that level 3-5 data is widely exposed externally – (Significant number of record)
EMERGENCY	• Any cyber threats to public and life safety systems • Compromise or loss of availability of systems responsible for the City's critical functions and infrastructure • Compromise of Department's high-criticality systems as identified in the Department's IT COOP • Malware affecting multiple Departments or spreading at a rapid rate on the network

During an emergency-level incident, communications will be managed by the Joint Information Center (JIC), a collaboration of the DT, DEM, and Mayor's Office PIOs, as well as the PIOs of any affected departments.

This plan is intended to be used by or in consultation with JIC. External emergency communications should not be sent without JIC approval, especially if media is the intended audience (and all external communications in an emergency event will eventually be broadcast by the media, even if that is not CCSF staff's intent).

To access this plan, please reach DEM Joint Information Center.

Appendix 7: Glossary

Term	Definition
Baselining	Monitoring resources to determine typical utilization patterns so that significant deviations can be detected.
Cyber Attack	Criminal activity conducted using computers and the Internet. This includes a broad range of activity from downloading illegal music files to monetary theft, fraud, distributing malware, posting confidential information, and identity theft.
Cyber Crime	Criminal activity conducted using computers and the Internet. This includes a broad range of activity from downloading illegal music files to monetary theft, fraud, distributing malware, posting confidential information, and identity theft
Cyber Incident	An event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or data. A cyber incident may impact organizational operations (including mission, capabilities, or reputation). A significant cyber incident is an incident (or group of related incidents) that is likely to result in demonstrable harm to public health and safety, critical functions, civil liberties, economy and/or community.
Cyber Security	The process of protecting information and systems by preventing, detecting, and responding to threats and attacks.
Cyber Terrorism	Any premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups. A cyber terrorist attack is designed to cause physical violence or extreme financial harm.
Data Breach	A data breach is the release of nonpublic information to an untrusted entity. Nonpublic data Includes but not limited to: Medical (HIPAA), Financial (PCI/Nacha), Identity (PII), Legal/law enforcement data
Denial of Service (DOS) Attack	The prevention of authorized access to a system resource or the delaying of system operations and functions. This often involves cyber criminals generating a large volume of data requests. A Distributed Denial of Service (DDOS) employs thousands of hijacked computers or internet-connected devices to deliver the data requests.
Domain Name System (DNS)	Helps users find their way around the Internet. Each computer and device on the Internet has its own unique address – much like a long, complicated phone number known as the Internet Protocol (IP) Address. DNS allows for a simple name (e.g., Amazon) to be used instead of the IP Address.
Event	Any observable occurrence in a network or system. False Positive: An alert that incorrectly indicates that malicious activity is occurring.
Exploit	A piece of software or sequence of commands that take advantage of a bug or vulnerability in order to cause unintended or unanticipated behavior to occur on computer software or hardware. A Zero Day Exploit is a new, previously unknown vulnerability
Hacktivist	A hacker who attacks information systems with the intent to advance a particular social or political agenda.
Hostname	A hostname is the label assigned to a device (a *host*) on a network and is used to distinguish one device from another on a specific network or over the internet.
Intrusion Detection and Prevention System (IDPS)	Software that automates the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents and attempting to stop detected possible incidents [2]

Term	Definition
Malware	A virus, worm, Trojan horse, or other program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system.
Patch	An update released by a software manufacturer to fix bugs or remove vulnerabilities in existing programs.
Phishing	Soliciting private information from customers or members of a business, bank or other organization in an attempt to fool them into divulging confidential personal and financial information. People are lured into sharing usernames, passwords, account information or credit card numbers, usually by an official-looking message in an email or a pop-up advertisement that urges them to act immediately, usually by clicking on a link provide.
Social Engineering	A euphemism for non-technical or low technology means (such as lies, impersonation, tricks, bribes, blackmail and threats) used to attack information systems via an organization's staff.
Threat	Natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property. For cyber threats this also includes the potential source of an adverse incident.
Vulnerability	Physical feature or operational attribute that renders an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard. For cyber, this also means a weakness in a system, application, or network that is subject to exploitation or misuse.