ESF COORDINATOR:	Information Systems Manager
LEAD AGENCIES:	Administrative Services Department
SUPPORT AGENCIES:	Shoreline Police Department All City Departments Emergency Operations Center King County Emergency Coordination Center Washington State Emergency Management Division

Introduction

Section 1.01 Purpose

(a) This annex discusses policies, organization, actions, and responsibilities for a coordinated, multidisciplinary, broad-based approach to prepare for, respond to, and recover from cyber-related "Incidents of City Significance" impacting critical City processes and the City economy. To accomplish this, this annex establishes a structure for a systematic, coordinated, unified, timely and effective investigative response to threats or acts of Cyber Attack within the City.

Section 1.02 Scope

(a) This annex is a strategic document that provides planning guidance and outlines operational concepts for the implementation of investigative response to a threatened or actual Cyber Attack incident within the City.

(b) This document applies to all threats or acts of Cyber Attack that require response and recovery actions within the City of Shoreline.

(c) This annex describes the framework for City cyber incident response coordination among City departments and agencies.

(d) This framework may be utilized in any Incident of City Significance with cyber-related issues, including significant cyber threats and disruptions; crippling cyber attacks against the Internet or critical infrastructure information systems; technological emergencies; or City declared disasters.

(e) This annex describes the specialized application of the City's CEMP to cyber-related Incidents of City Significance. Cyber-related Incidents of City Significance may result in activation of both ESF #2 – Communications, the Cyber Incident Annex, and Terrorism Incident Annex.

(f) The City contracts with the King County Sheriff's Office to provide the City with police services. This department operates and maintains their information technology systems.

Section 1.03 Situation

(a) An information security event usually results from man-made technological cyber attack that produces damage and results in a large number of requests for services to mitigate the cyber attack. The City, when notified of an emergency situation at the City level, will monitor the situation and provide assistance as resources allow.

(b) Until such time as an incident is determined to be an act of terrorism, response operations will be implemented under the City of Shoreline CEMP.

Section 1.04 Assumptions

(a) The Information Systems Manager, will advise and provide guidance to the City Manager or designee regarding the City's response to a potential threat or actual occurrence of a Cyber Attack incident.

(b) The City may be heavily dependent on outside agencies and vendor assistance in order to adequately respond to Cyber Attack's.

(c) The Cyber security Preparedness and the National Cyber Alert System will provide regular updates to the City on Cyber threats and may provide assistance with response and recovery, as appropriate.

(d) The occurrence or threat of multiple cyber incidents may significantly hamper the ability of responders to adequately manage the cyber incident.

(e) A debilitating infrastructure attack could impede communications needed for coordinating response and recovery efforts.

(f) Cyberspace is largely owned and operated by the private sector; therefore, the authority of the City Government to exert control over activities in cyberspace is limited.

(g) The Police Department will be notified of all cyber incidents that may be a criminal act.

Section 1.05 Policies

(a) All activities within the Cyber Attack Annex will be conducted in accordance with the National Incident Management System (NIMS) and the National Response Framework (NRF) and will utilize the Incident Command System (ICS).

(b) As a signatory of the King County Regional Disaster Plan and through local mutual aid agreements, the City will make resources available to other jurisdictions through the Zone 1 Emergency Coordinator, and King County Emergency Coordination Center (KC ECC), whenever possible.

(c) The Administrative Services Department will coordinate activities within this plan. It is anticipated that the City will relinquish criminal investigative authority to the Federal Bureau of Investigation (FBI) for Terrorism Incidents.

Article II. Definitions

Word	Definition
Terrorism	Terrorism is the systematic use of terror (imposing fear), especially as a means of coercion. At present, there is no internationally agreed definition of terrorism. Common definitions of terrorism refer only to those acts which are (1) intended to create fear (terror), (2) are perpetrated for an ideological goal (as opposed to a materialistic goal or a lone attack), and (3) deliberately target (or disregard the safety of) non-combatants. Some definitions also include acts of unlawful violence or war. A person who practices terrorism is a terrorist. Acts of terrorism are criminal acts according to United Nations Security Council Resolution 1373 and the domestic jurisprudence of almost all nations.
FBI – Joint Operations Center (JOC)	A centralized operations center established by the FBI Field Office/Resident Agent during terrorism-related incidents to provide a single point of direction, control, and coordination for emergency response operations. The JOC resolves conflicts in prioritization of resource allocations involving Federal assets. The location of the JOC will be based upon the location of the incident and current threat specific information.
Joint Information Center (JIC)	A combined public information center that serves two or more levels of government or Federal, State, and local agencies. During a terrorist incident, the FBI will establish and maintain this facility.
Cyber Incident	A disruption, intrusion, or compromise resulting from an adverse event whose actions results in harm or significant threat of harm to the availability, integrity, and confidentiality of an organization's data or computing assets.

Viruses	Self-replicating code that makes copies of itself and distributes it to other computers, files or programs.
Spyware or Trojans	Programs that appear to be benign, but have hidden functions or purposes once introduced into a system or network.
Worms	Self-replicating programs that do not require a host program to infect.
Mobile Code	Software that is transmitted from a remote to local system.
Blended Attacks	Code that has multiple methods to spread, such as the Nimda "worm". The Nimba worm used: email, Windows shares, web servers, and web clients.
Spam	Email spam is not usually elevated to the severity of a computer incident unless it is determined to carry a malicious payload or be part of a reconnaissance effort.
Denial of Service (DoS)	In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting your computer and its network connection, or the computers and network of the sites you are trying to use, an attacker may be able to prevent you from accessing email, websites, online accounts (banking, etc.), or other services that rely on the affected computer.

Article III. Concept of Operations

Section 3.01 General

(a) The Administrative Services Department is the lead agency for the coordination of activities within this Cyber Attack Annex with federal, state, and county law enforcement agencies and IT departments.

(b) Cyber security incidents are identified and reported by the City Departments. In response to an incident, the City Departments involved in the response will assess the situation to identify any needs and requirements, in consultation with the Information Technology Manager.

(c) A cyber-related Incident of City Significance may take many forms: an organized cyber attack, an uncontrolled exploit such as a virus or worm, a natural disaster with significant cyber consequences, or other incidents capable of causing extensive damage to critical infrastructure or key assets.

(d) Large-scale cyber incidents may overwhelm government and private-sector resources by disrupting the Internet and/or taxing critical infrastructure information systems. Complications from disruptions of this magnitude may threaten lives, property, the economy, and national security. Rapid identification, information exchange, investigation, and coordinated response and remediation often can mitigate the damage caused by this type of malicious cyberspace activity.

(e) The FBI has authority for the criminal investigation of all potential or actual terrorist incidents within the United State.

(f) An incident command post will be established for the coordination of field operations. The unified command structure will be used when multiple departments/agencies are responding to an event.

(g) Warning

(i) Every incident is different. There may or may not be warning of a potential cyber attack. Factors involved range from intelligence gathered from various law enforcement or intelligence agency sources to an actual notification from the terrorist organization or individual.

(ii) The warning or notification of a potential cyber attack incident could come from many sources; therefore, open but secure communication among local, State, and Federal law enforcement agencies and emergency response officials is essential.

(iii) The Information Technology Manger notifies the City Manager, Emergency Management Coordinator, Police Chief, and other designed officials of cyber-related incidents. The activities described in this annex are implemented when a cyber-related Incident of City Significance is imminent or underway. The Administrative Services Director or Emergency Management Coordinator may determine a cyber-related Incident is of City Significance.

(h) Notification and Activation

(i) The City EOC may be fully activated upon the receipt of information from the Cyber security Preparedness and the National Cyber Alert System and that warrants a coordinated response.

(ii) Based upon the information received, the Administrative Services Director or Emergency Management Coordinator will determine the operational level of the EOC and notify the Primary and/or Support Agencies for each of the EOC sections, as appropriate.

(i) Communications

(i) Communications and alerts will be made utilizing standard communications methods outlined in ESF 2 Communications.

(ii) Pre-Incident Phase:

1) A credible or significant threat may be presented in verbal, written, intelligence-based or other form.

2) The Administrative Services Department maintains contact listing of local and regional Information Technology partners.

3) City requests for assistance from Regional, State and Federal agencies will be coordinated through the City EOC. During the course of a threat assessment, consequences may become imminent or occur that causes the Administrative Services Director, or delegate, to direct resources to implement in part or in total the actions as described in this Annex.

(iii) Trans-Incident (Situations involving a transition from a threat to an act of terrorism):

1) The City Administrative Services Department will contact City agencies, as appropriate, and provides the initial notification to other regional information technology departments, City Departments of the confirmed presence of unusual cyber activity.

2) As the situation warrants, the Administrative Services Director will coordinate with the City Manager and EM Coordinator regarding the need to activate the City's Continuity of Operations (COOP) and/or Emergency Operations plans, as appropriate.

(iv) Post-Incident

1) Once an incident has occurred, the Administrative Services Director, or delegate, will provide a Liaison to the respective local EOC and/or the FBI JOC, as needed.

2) The Information Technology Manager will assist in conducting an After Action Report (AAR).

(v) Deactivation

1) If an act of Cyber Attack does not occur, the responding elements will deactivate when the Administrative Services Director, in consultation with the EM Coordinator and City Manager, issues a cancellation notification to the appropriate agencies. Agencies will coordinate with the EOC Operations Officer and deactivate according to establish SOPs.

2) If an act of Cyber Attack does occurs, then each EOC section deactivates at the appropriate time according to established SOPs. Following section deactivation, operations by individual City agencies may continue, in order to support the affected local governments.

Section 3.02 Organization

(a) The Administrative Services Department is the lead agency for the coordination of Cyber Attack activities within the City.

(b) The Administrative Services Director or his/her designee will designate an Emergency Operations Center (EOC) representative to coordinate field operations and resources with federal agencies.

(c) The Administrative Services Department will follow all departmental policies and procedures relating to chain of command and on-scene management and will utilize the ICS.

(d) A unified command structure will normally be established when law enforcement agencies from outside the City are assisting with operational activities within the City.

(e) The FBI has authority for the criminal investigation, crime scene, and apprehension of those responsible for potential or actual terrorist incidents. The Police Chief or designee will coordinate activities with the FBI.

Section 3.03 Actions

(a) Preparedness:

(i) Conduct planning with other Information Technology support agencies and other emergency support functions to refine Cyber Attack operations.

(ii) Prepare and maintain emergency operating procedures, resource inventories, personnel rosters and resource mobilization information necessary for implementation of the responsibilities of the lead agency,

(iii) Assign and schedule sufficient personnel to implement mass care tasks for an extended period of time,

(iv) Conduct vulnerability analysis at critical facilities and make recommendation to improve the physical security

(v) Ensure lead agency personnel are trained in their responsibilities and duties,

(vi) Develop and implement emergency response strategies relating to terrorism response

(vii) Develop and present training courses for terrorism response.

(viii) Maintain liaison with support agencies,

(ix) Conduct All Hazards exercises involving Cyber Attack response.

(b) Response:

(i) See Section 3.01 Concept of Operations of this plan for additional response information.

(ii) Coordinate operations in the Shoreline EOC and/or at other locations as required,

(iii) Develop, prioritize and implement strategies for the initial response to EOC requests.

(iv) Establish communications with appropriate field personnel to ensure readiness for timely response,

(v) Participate in EOC briefings, development of Incident Action Plans and Situation Reports, and meetings,

(vi) Coordinate with support agencies, as needed, to support emergency activities,

(vii) Obtain other resources through the Law Enforcement State Wide Mobilization and Mutual Aid Plan, Statewide Emergency Management Mutual Aid and Assistance Agreement and/or the Regional Mutual Aid Agreements,

(viii) Coordinate with other jurisdictions to obtain resources and facilitate an effective emergency response among all participating agencies,

(ix) Monitor and direct response activities to include prepositioning for response/relocation due to the potential impacts of the emergency situation.

(x) Pre-position response resources when it is apparent that resources may be necessary.

(c) Recovery

(i) Recovery activities for this ESF are covered in the Shoreline Disaster Recovery Plan.

(d) Mitigation

(i) Mitigation activities for this ESF are covered in the Multijurdictional Hazard Mitigation.

Article IV. Responsibilities

Section 4.01 Lead Agency

(a) Administrative Services Department

(i) Provide support to the Emergency Management Coordinator in the dissemination of emergency warning information to the public and in the operation of the EOC.

(ii) Make recommendations concerning area cyber security and cyber incident response.

(iii) Coordinate Cyber Attack response activities with other departments and agencies.

Section 4.02 Support Agency

(a) Emergency Operations Center

(i) Coordinate response activities with the FBI and the Police Department.

(ii) Implement the City's Comprehensive Emergency Management Plan and Cyber Attack Annex.

(iii) Coordinate information between various departments within the City and external agencies to ensure efficient and accurate communication.

(iv) Submit and coordinate requests for additional resources to the Z1 ECC, KC ECC, or Washington Emergency Management Division (WA EMD).

(v) Assist the City Manager to ensure continuity of government in the event of a Cyber Attack incident.

(vi) Activate the Intelligence function within the ICS if applicable and advised to do so by the police department

(vii) Notify the Washington State Fusion Center.

(b) King County Emergency Coordination Center

(i) Communicate with Zone 1, 3, and 5 ECCs and cities, WA EMD and all related agencies regarding Cyber Attack response activities.

(ii) Coordinate requests for resources with the above entities and facilitate the equitable distribution of available resources.

(c) Washington Emergency Management Division

(i) Provide coordination of State resources to provide support, as appropriate, when all local, regional, and county resources have been expended.

(ii) Facilitate the requisition of resources from other states through the Emergency Management Assistance Compact (EMAC).

(iii) Request and coordinate Federal resources through the Department of Homeland Security.

(d) All City Departments

(i) Assist in Cyber Incident response activities, as requested by the Administrative Services Department.

(ii) Report any unusually activity on information technology systems through established communication channels.

Article V. Appendices

(a) Cyber Incident Triggers

Article VI. References

(a) National Response Framework

(b) Emergency Management Assistance Compact

(c) National Cyber Security Division

Appendix A – Cyber Incident Triggers

Severity levels help determine the extent of response to security incidents by individual City Departments or a City-wide incident response team. The different Levels should be one element that it considered, when determining at what level the City should respond.

MINOR

Possible Incursion on critical or non-critical system; detection of precursor to a focused attack; believed threat of an imminent attack. IT responders see potential for citywide problems.

1. **Is public perception of City government services at risk? If there is imminent danger of** modification of the public's confidence of the City to provide leadership and efficient City services then assign the incident
2. **Is there an incursion on a non-critical system without the threat of attacking others?** If the incident involves an incursion on non-critical system without the threat of attacking others, then assign the incident
3. **Does the City have a security problem that has been identified in a public forum?** If the incident involves an alleged City security problem that has been identified in a public forum such as new vulnerabilities in operating systems or other applications in use in the City, then assign the incident

MODERATE

Threat of a future attack; detection of reconnaissance…some aspects of incident raise concerns for the IT responders.

1. **Does the incident involve malware that is a known threat?** If the incident involves spam, spyware or other malware that could potentially be a future threat to Citywide systems (either because it is possibly reconnoitering, monitoring or using City equipment as "wartime reserves"), then assign the incident

MAJOR

Incident could have long-term effects on business; incident affects critical systems, impacts entities outside the City of Shoreline, and/or involves multiple City Departmental systems.

1. **Is there a threat to physical safety?** If the incident involves a threat to any person's physical safety.
2. **Is sensitive data, personally identifiable data, or intellectual property at risk?** If there is imminent danger (the act is in progress) that confidential information can be read, modified, or destroyed by an unauthorized entity or the disclosure or access already occurred, then assign the incident
3. **Is business continuity at risk?** If there is imminent danger of disruption of business due to security issues or malicious acts or the disruption is in progress, then assign the incident
4. **Does the incident harm entities outside the City of Shoreline?** If there is danger of harm to an outside entity from the incident, such as a Denial of Service (DoS) attack, then assign the incident
5. **Are multiple City systems involved?** If the incident includes multiple systems, then assign the incident