THREAT AND HAZARD IDENTIFICATION AND RISK ASSESSMENT (THIRA)

May 2019

CITY OF COCOA

Prepared by the East Central Florida Regional
Planning Council

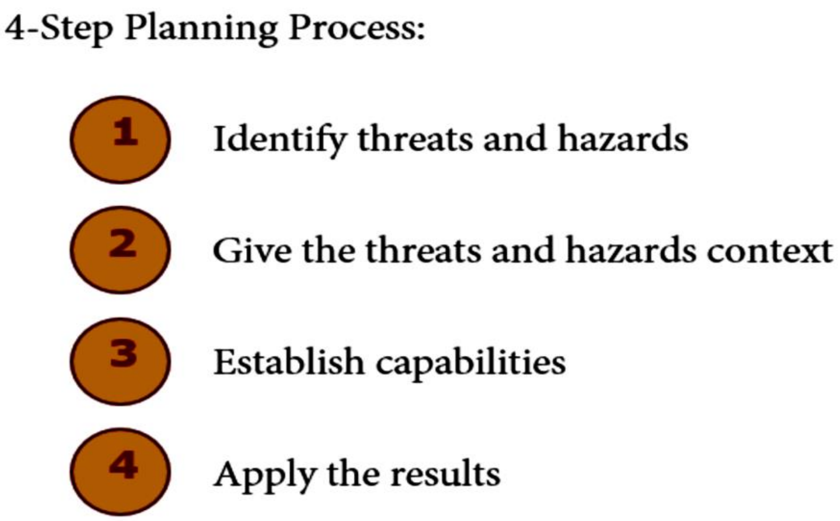
Contents

Introduction

The City of Cocoa is at risk to a variety of natural and non-natural hazards. Preventing, protecting from, mitigating, responding to, and recovering from hazards and threats requires extensive coordination among City agencies and local partners. The City's Fire Department leads that coordination with the goal of developing, maintaining, and sustaining a citywide, comprehensive, all hazard, risk-based emergency management program that engages the whole community.

This Threat and Hazard Identification and Risk Assessment (THIRA) Report is the result of a collaborative planning process. It is compliant with the U.S. Department of Homeland Security (DHS) Comprehensive Preparedness Guide (CPG) 201, Third Edition, released in May 2018, which outlines a process to help communities identify capability targets and resource requirements necessary to address anticipated and unanticipated risks. The result of the THIRA process is an organized evaluation of vulnerability and implementation measures based on the necessary capabilities to deal with the hazards/threats of most concern.

The THIRA follows a four-step process, as described in Comprehensive Preparedness Guide 201, third Edition:



4-Step Planning Process:

1 Identify threats and hazards

2 Give the threats and hazards context

3 Establish capabilities

4 Apply the results

1. Identify the Threats and Hazards of Concern. Based on a combination of past experience, forecasting, expert judgment, and other available resources, communities identify a list of the threats and hazards of primary concern to the community.

2. Give the Threats and Hazards Context. Communities describe the threats and hazards of concern, showing how they may affect the community.

3. Establish Capability Targets. Communities assess each threat and hazard in context to develop a specific capability target for each relevant core capability. The capability target defines success for the capability.

4. Apply the Results. Communities estimate the required resources per core capability to meet the capability targets.

The THIRA helps communities determine what they need to prepare for, what resources they require, and what their current gaps are. Communities can use this information to help them efficiently build and sustain preparedness capabilities.

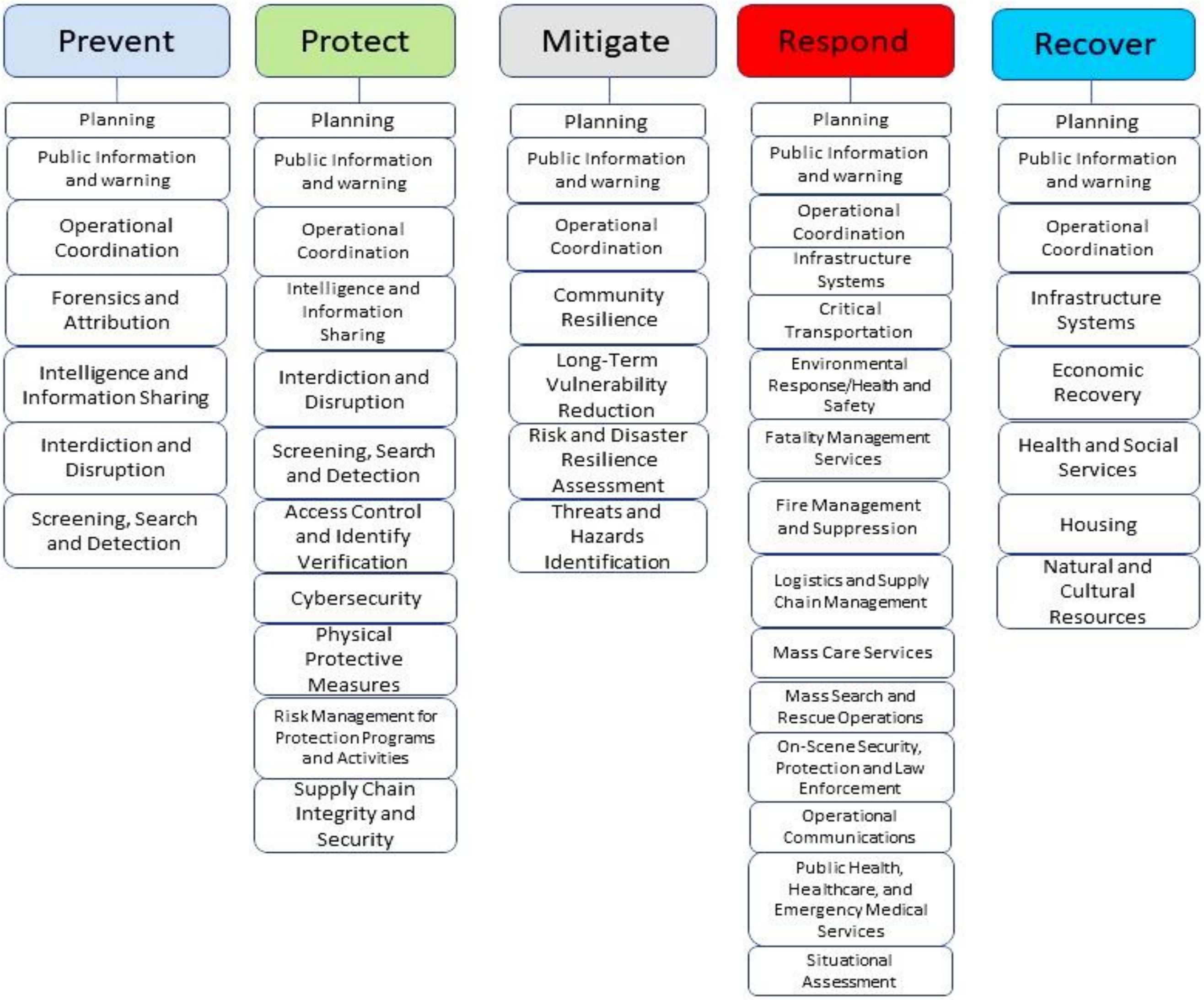
Goal Setting

Presidential Policy Directive 8: National Preparedness sets forth a national goal for “a secure and resilient Nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk”. To achieve this, the National Preparedness Goal identifies 32 necessary core capabilities. The City of Cocoa reviewed the National Preparedness Goal and through discussion established a more refined set of desired outcomes for the City based on the 32 core capabilities.

This chart below contains the 32 core capabilities identified in the National Preparedness Goal and is intended to assist everyone who has a role in achieving all of the elements in the Goal.

These capabilities are referenced in many national preparedness efforts, including the National Planning Frameworks. The Goal grouped the capabilities into five mission areas, based on where they most logically fit. Some fall into only one mission area, while some others apply to several mission areas.

National Preparedness Core Capabilities



Prevent

- Planning
- Public Information and warning
- Operational Coordination
- Forensics and Attribution
- Intelligence and Information Sharing
- Interdiction and Disruption
- Screening, Search and Detection

Protect

- Planning
- Public Information and warning
- Operational Coordination
- Intelligence and Information Sharing
- Interdiction and Disruption
- Screening, Search and Detection
- Access Control and Identify Verification
- Cybersecurity
- Physical Protective Measures
- Risk Management for Protection Programs and Activities
- Supply Chain Integrity and Security

Mitigate

- Planning
- Public Information and warning
- Operational Coordination
- Community Resilience
- Long-Term Vulnerability Reduction
- Risk and Disaster Resilience Assessment
- Threats and Hazards Identification

Respond

- Planning
- Public Information and warning
- Operational Coordination
- Infrastructure Systems
- Critical Transportation
- Environmental Response/Health and Safety
- Fatality Management Services
- Fire Management and Suppression
- Logistics and Supply Chain Management
- Mass Care Services
- Mass Search and Rescue Operations
- On-Scene Security, Protection and Law Enforcement
- Operational Communications
- Public Health, Healthcare, and Emergency Medical Services
- Situational Assessment

Recover

- Planning
- Public Information and warning
- Operational Coordination
- Infrastructure Systems
- Economic Recovery
- Health and Social Services
- Housing
- Natural and Cultural Resources

The following statements represent an ideal condition of the whole community's capability to prevent, protect against, mitigate, respond to, and recover from the threats and hazards of most concern.

1. Planning

Conduct a systematic process engaging the whole community as appropriate in the development of executable strategic, operational, and/or tactical-level approaches to meet defined objectives.

2. Public Information and Warning

Deliver coordinated, prompt, reliable, and actionable information to the whole community through the use of clear, consistent, accessible, and culturally and linguistically appropriate methods to effectively relay information regarding any threat or hazard, as well as the actions being taken and the assistance being made available, as appropriate.

3. Operational Coordination

Establish and maintain a unified and coordinated operational structure and process that appropriately integrates all critical stakeholders and supports the execution of core capabilities.

4. Forensics and Attribution

Conduct forensic analysis and attribute terrorist acts (including the means and methods of terrorism) to their source, to include forensic analysis as well as attribution for an attack and for the preparation for an attack in an effort to prevent initial or follow-on acts and/or swiftly develop counter-options.

5. Intelligence and Information Sharing

Provide timely, accurate, and actionable information resulting from the planning, direction, collection, exploitation, processing, analysis, production, dissemination, evaluation, and feedback of available information concerning physical and cyber threats to the United States, its people, property, or interests; the development, proliferation, or use of WMDs; or any other matter bearing on U.S. national or homeland security by local, state, tribal, territorial, federal, and other stakeholders. Information sharing is the ability to exchange intelligence, information, data, or knowledge among government or private sector entities, as appropriate.

6. Interdiction and Disruption

Delay, divert, intercept, halt, apprehend, or secure threats and/or hazards.

7. Screening Search and Detection

Identify, discover, or locate threats and/or hazards through active and passive surveillance and search procedures. This may include the use of systematic examinations and assessments, bio surveillance, sensor technologies, or physical investigation and intelligence.

8. Access Control and Identity Verification

Apply and support necessary physical, technological, and cyber measures to control admittance to critical locations and systems.

9. Cybersecurity

Protect (and if needed, restore) electronic communications systems, information, and services from damage, unauthorized use, and exploitation.

10. Physical Protective Measures

Implement and maintain risk-informed countermeasures, and policies protecting people, borders, structures, materials, products, and systems associated with key operational activities and critical infrastructure sectors.

11. Risk Management for Protection Programs and Activities

Identify, assess, and prioritize risks to inform Protection activities, countermeasures, and investments.

12. Supply Chain Integrity and Security

Strengthen the security and resilience of the supply chain.

13. Community Resilience

Enable the recognition, understanding, communication of, and planning for risk and empower individuals and communities to make informed risk management decisions necessary to adapt to, withstand, and quickly recover from future incidents

14. Long–term Vulnerability Reduction

Build and sustain resilient systems, communities, and critical infrastructure and key resources lifelines so as to reduce their vulnerability to natural, technological, and human-caused threats and hazards by lessening the likelihood, severity, and duration of the adverse consequences

15. Risk and Disaster Resilience Assessment

Assess risk and disaster resilience so that decision makers, responders, and community members can take informed action to reduce their entity's risk and increase their resilience.

16. Threats and Hazards Identification

Identify the threats and hazards that occur in the geographic area; determine the frequency and magnitude; and incorporate this into analysis and planning processes so as to clearly understand the needs of a community or entity.

17. Critical Transportation

Provide transportation (including infrastructure access and accessible transportation services) for response priority objectives, including the evacuation of people and animals, and the delivery of vital response personnel, equipment, and services into the affected areas.

18. Environmental Response/Health and Safety

Conduct appropriate measures to ensure the protection of the health and safety of the public and workers, as well as the environment, from all-hazards in support of responder operations and the affected communities.

19. Fatality Management Services

Provide fatality management services, including decedent remains recovery and victim identification, working with local, state, tribal, territorial, insular area, and federal authorities to provide mortuary processes, temporary storage or permanent internment solutions, sharing information with mass care services for the purpose of reunifying family members and caregivers with missing persons/remains, and providing counseling to the bereaved.

20. Fire Management and Suppression

Provide structural, wildland, and specialized firefighting capabilities to manage and suppress fires of all types, kinds, and complexities while protecting the lives, property, and the environment in the affected area.

21. Infrastructure Systems

Stabilize critical infrastructure functions, minimize health and safety threats, and efficiently restore and revitalize systems and services to support a viable, resilient community.

22. Logistics and Supply Chain Management

Deliver essential commodities, equipment, and services in support of impacted communities and survivors, to include emergency power and fuel support, as well as the coordination of access to community staples. Synchronize logistics capabilities and enable the restoration of impacted supply chains.

23. Mass Care Services

Provide life-sustaining and human services to the affected population, to include hydration, feeding, sheltering, temporary housing, evacuee support, reunification, and distribution of emergency supplies.

24. Mass Search and Rescue Operations

Deliver traditional and atypical search and rescue capabilities, including personnel, services, animals, and assets to survivors in need, with the goal of saving the greatest number of endangered lives in the shortest time possible.

25. On-scene Security, Protection, and Law Enforcement

Ensure a safe and secure environment through law enforcement and related security and protection operations for people and communities located within affected areas and also for response personnel engaged in lifesaving and life-sustaining operations.

26. Operational Communications

Ensure the capacity for timely communications in support of security, situational awareness, and operations by any and all means available, among and between affected communities in the impact area and all response forces.

27. Public Health, Healthcare, and Emergency Medical Services

Provide lifesaving medical treatment via Emergency Medical Services and related operations and avoid additional disease and injury by providing targeted public health, medical, and behavioral health support, and products to all affected populations.

28. Situational Assessment

Provide all decision makers with decision-relevant information regarding the nature and extent of the hazard, any cascading effects, and the status of the response.

29. Economic Recovery

Return economic and business activities (including food and agriculture) to a healthy state and develop new business and employment opportunities that result in an economically viable community.

30. Health and Social Services

Restore and improve health and social services capabilities and networks to promote the resilience, independence, health (including behavioral health), and well-being of the whole community.

31. Housing

Implement housing solutions that effectively support the needs of the whole community and contribute to its sustainability and resilience.

32. Natural and Cultural Resources

Protect natural and cultural resources and historic properties through appropriate planning, mitigation, response, and recovery actions to preserve, conserve, rehabilitate, and restore them consistent with post-disaster community priorities and best practices and in compliance with applicable environmental and historic preservation laws and executive orders.

Hazard Identification

Identified Hazards and Threats

Several City and regional emergency management and planning documents were reviewed to identify a comprehensive list of hazards for consideration. These documents address both natural and human caused hazards that have the potential to impact the City of Cocoa. Many of these documents estimate the impacts that result from the identified hazards.

Threats and Hazards

Category	Threat/Hazard	Context
Man-Made or Technological	Airplane Accident	Aircraft accidents in Cocoa can result from an aircraft experiencing trouble or from mid-air collisions between aircraft flying over or near Cocoa as they approach the Area Airports (Melbourne, Merritt Island, Rockledge, Titusville).
Man-Made or Technological	Civil Disturbance	The public may be negatively impacted by a civil disturbance. If a civil disturbance were to occur during a major event, bystanders may be injured or killed. Property is at risk to a civil disturbance. Rioters may damage both private and public property, disrupting the ability to respond to the situation and causing damages in the hundreds of thousands of dollars. Florida has experienced seven major riots, beginning with the 1923 Rosewood riot, then 1967 Tampa riots, 1980 Miami riots, 1982 Miami riots, 1987 Tampa riots, 1989 Tampa riots, and most recently the 1996 St. Petersburg riots.
Man-Made or Technological	Cyber Attack	A successful cyber-attack at the local level may negatively impact the public's ability to conduct business with the City. It is possible that they would be unable to pay utility or tax bills online. On a national scale, increased online control of critical infrastructure means greater vulnerability of electrical power grids, water and transportation systems, oil pipelines, refineries and power generation plants. Should a cyber-attack take down the City internet/intranet system, city programmatic activities may experience a minor impact. Cyber infrastructure enables storage and transfer of massive amounts of knowledge to enable planning, resource allocation, personnel

Category	Threat/Hazard	Context
		deployment, and coordination of emergency situations. The Cocoa Information Technology Department would activate its COOP and Disaster Recovery Plan in this situation.
Man-Made or Technological	Radiological Launch Event	A Major Radiological Source (MRS) is defined as Nuclear Reactors and other devices with a potential for criticality and radioactive materials to be launched which requires presidential nuclear approval per "National Security Council/Presidential Directive No. 25," paragraph 9. Examples would include, but not limited to, Radioisotope Power Systems (RPSs), and Radioisotope Heater Units (RHUs). The RHU produces electrical power by converting heat from the decay of Plutonium 238 (PUO_2). The design of the RHU is such that they will survive intact and prevent the release of Plutonium for most launch accident scenarios. Worst case scenarios for the possible release of Plutonium involve either an on-pad or low-altitude launch catastrophic event. The Challenger Space Shuttle exploded over Cape Canaveral, Florida in 1986 just a few minutes into the launch. The Columbia Space Shuttle exploded upon re-entry over Texas in 2003. On September 1, 2016, an unmanned Space-X rocket blew up on the launch pad during testing at Kennedy Space Center, Florida.
Man-Made or Technological	Rail Accident	The City of Cocoa has commercial rail lines operating through the heart of the city. Florida East Coast Railway and Amtrak both use the rail system. A rail incident presents a potential scene where wreckage, victims, and survivors may be strewn over a wide area. It can further be complicated by hazardous cargo. The City of Cocoa has experienced many vehicle versus train accidents at rail crossings, including

Category	Threat/Hazard	Context
		one which resulted in one fatality and a minor train derailment in November, 2017.
Natural	Freezing Weather	All of the City of Cocoa is vulnerable to winter storms. Being in the southern portion of the nation, we rarely experience severe winter storm events, however there were two extended cold periods in the 1980's that froze many of the orange groves. FEMA has recorded four severe winter freezes from 1977 - 2001. Historically the greatest impact of cold weather has been on the homeless population. Shelters have been opened during cold weather events for them. All of the City of Cocoa is vulnerable to freezing weather.
Natural	Flooding	According to FloodSmart.gov, all 50 states are at risk to flooding and flash floods. Flash floods are particularly dangerous because they can quickly sweep cars off roadways, causing injuries and causalities to people in its path. (The City of Cocoa does not experience true "flash flooding"). In addition to life safety, property can be damaged by just an inch of water (FloodSmart.gov). Homeowners insurance and renter's insurance does not cover flooding. A separate policy under the NFIP must be purchased. Citizens without flood insurance may not receive any assistance to repair their homes and property following an event. The City of Cocoa has 8,914 structures in the 100-year floodplain. Property in low-lying areas or Special Flood Hazard Areas (100-year floodplain) are susceptible to damage from flooding (FloodSmart). Floods can destroy homes and businesses, erode property along creeks and rivers, and washout roads and bridges. In some cases, flooding is a secondary hazard from a hurricane event, such as the case with Hurricane Irma. According to FEMA, flooding is the costliest natural hazard in the U.S. and can cause long-term adverse psychological impacts. The City of Cocoa has

Category	Threat/Hazard	Context
		experienced two major flood events not related to hurricanes since 2005 resulting in over $1,020,000 in insured flood losses.
Man-Made or Technological	Hazardous Materials and Nuclear Incidents	Large amounts of hazardous materials, including radioactive materials, are transported through and around the city daily by rail, truck transport, and via the intercoastal waterways. As of 2018, the City of Cocoa had 41 facilities reported in E-Plan that stored hazardous materials that are subject to Section 302, Section 311, and Section 312 of the Superfund Amendments and Reauthorization Act (SARA) title III, Emergency Planning and Community Right-to-Know Act (EPCRA) within their facility. The City of Cocoa is not within 50-mile limit for the ingestion pathway of the three nuclear power plants located in the state. The proximity of the Kennedy Space Center and the Trident Nuclear Submarine Basin at Port Canaveral in nearby Brevard County, however, does pose some small risk to the City should a catastrophic nuclear incident occur at either of those locations. Across the US, there were 2,518 truck accidents involving hazardous cargo in 2010. These resulted in 34 injuries, nine deaths and almost $80 million in damages.
Natural	Tropical Storm/ Hurricanes	The City of Cocoa's worst hurricane season was 2004. Hurricane Charley, Frances and Jeanne impacted the City of Cocoa, back-to-back. Since 1953, the City of Cocoa has been impacted by 15 hurricanes. Most recently, Hurricane Matthew in 2016 and Hurricane Irma in 2018, which resulted in the failure of a main waterline serving over 85,500 customers.
Natural	Tornadoes and Severe Weather	Tornadoes pose a great risk to people and structures. City of Cocoa is at risk of the impacts of a tornado. From 1996 to 2013, the City of Cocoa had one confirmed tornado events, responsible for over $450,000 in property damage. No fatalities

Category	Threat/Hazard	Context
		and no injuries were reported. (Section V, NOAA Climatic Data Center). Tornadoes can reach wind speeds over 200mph, (although the most powerful tornado to impact the City of Cocoa was an EF1) lifting homes and businesses off of their foundations, crippling infrastructure and creating automobile sized missiles.
Natural or Man-Made	Wildfire	Between 2000 -2008, the average number of wildfires per year was 129. People and their property are at risk to the impacts of a wildfire. Wildfires can burn down trees, vegetation, homes and businesses. Smoke from wildfires can be detrimental to the health of citizens living in close proximity to the fires. Smoke and ash from wildfires can obscure vision and cause extended road closures. Wildfires can destroy public and private property, ravish parklands, and disrupt the service of critical utilities. Both forested and urban areas are at risk to wildfires. Brevard County has experienced six wildfires resulting in a Disaster Declaration since 1998. The 1998 wildfires resulting in 52 injuries and $200,000,000 in damages.

The City of Cocoa rated natural hazards through a qualitative analysis of probability and impact to people and property based on the scale of the hazard. The probability of occurrence of a hazard is indicated by a probability factor based on likelihood of annual occurrence:

- High—Hazard event is likely to occur within 25 years (Probability Factor = 3).

- Medium—Hazard event is likely to occur within 100 years (Probability Factor =2).

- Low—Hazard event is not likely to occur within 100 years (Probability Factor =1).

- No exposure—There is no probability of occurrence (Probability Factor = 0).

Hazard impacts were assessed in three categories: impacts on people, impacts on property and impacts on the local economy. Numerical impact factors were assigned as follows:

• People—Values were assigned based on the percentage of the total *population exposed* to the hazard event. The degree of impact on individuals will vary and is not measurable, so the calculation assumes for simplicity and consistency that all people exposed to a hazard because they live in a hazard zone will be equally impacted when a hazard event occurs. It should be noted that planners can use an element of subjectivity when assigning values for impacts on people. Impact factors were assigned as follows:

- ○ High—50 percent or more of the population is exposed to a hazard (Impact Factor = 3).
- ○ Medium—25 percent to 49 percent of the population is exposed to a hazard (Impact Factor = 2).
- ○ Low—25 percent or less of the population is exposed to the hazard (Impact Factor = 1).
- ○ No impact—None of the population is exposed to a hazard (Impact Factor = 0).

• Property—Values were assigned based on the percentage of the total *property value exposed* to the hazard event:

- ○ High—30 percent or more of the total assessed property value is exposed to a hazard (Impact Factor = 3).
- ○ Medium—15 percent to 29 percent of the total assessed property value is exposed to a hazard (Impact Factor = 2).
- ○ Low—14 percent or less of the total assessed property value is exposed to the hazard (Impact Factor = 1).
- ○ No impact—None of the total assessed property value is exposed to a hazard (Impact Factor = 0).

• Economy—Values were assigned based on the percentage of the total *property value vulnerable* to the hazard event. Values represent estimates of the loss from a major event of each hazard in comparison to the total replacement value of the property exposed to the hazard.

- High—Estimated loss from the hazard is 20 percent or more of the total exposed property value (Impact Factor = 3).
- Medium—Estimated loss from the hazard is 10 percent to 19 percent of the total exposed property value (Impact Factor = 2).
- Low—Estimated loss from the hazard is 9 percent or less of the total exposed property value (Impact Factor = 1).
- No impact—No loss is estimated from the hazard (Impact Factor = 0).

The impacts of each hazard category were assigned a weighting factor to reflect the significance of the impact. These weighting factors are consistent with those typically used for measuring the benefits of hazard mitigation actions: impact on people was given a weighting factor of 3; impact on property was given a weighting factor of 2; and impact on the economy was given a weighting factor of 1.

The final total risk ranking of Natural Hazards is summarized in the table below.

Rank	Hazard Type	Risk Rating Score (Probability x Impact)	Category
1	Flooding	18	Medium
2	Tropical Storm/Hurricane	32	High
3	Severe Storm/Tornadoes	18	Medium
4	Wildfire	9	Low
5	Freezing Weather	3	Low

Technological Hazard Prioritization

Each technological hazard was reviewed for its potential to occur. Knowledge, concerns, and other pertinent information was utilized to determine a rating on each technological hazard whether it was rated as low, medium, high, or very high.

Technological Hazards Rating Criteria

Technological Hazards Ranking Criteria	Rating
An event is imminent. Experts have confirmed potential for occurrence.	Very High
An event is expected/probable. Experts have confirmed potential for occurrence.	High
An event is possible. Potential for occurrence is assumed but not verified.	Medium

An event is unlikely. Potential for occurrence is extremely limited.	Low

Technological Hazard Rating Results

Technological Hazard	Rating
Airplane Accident	Low
Hazardous Materials and Nuclear Incidents	High
Rail Accident	Medium
Radiological Launch Event	Medium
Civil Disturbance	Low
Cyber Attack	High

Human Caused Threat Prioritization

Each human caused threat was reviewed for its potential to occur. The Stakeholder Group shared knowledge, concerns, and other pertinent information to come to a consensus on rating each human caused threat as low, medium, high, or very high.

Human Caused Threat Rating Criteria

Human Caused Threat Ranking Criteria	Rating
The likelihood of a threat, weapon, and tactic being used against a site or building is **imminent**. Internal decision makers and/or external law enforcement and intelligence agencies determine *the threat is credible*.	Very High
The likelihood of a threat, weapon, and tactic being used against a site or building is **expected**. Internal decision makers and/or external law enforcement and intelligence agencies determine *the threat is credible*.	High
The likelihood of a threat, weapon, and tactic being used against a site or building is **possible**. Internal decision makers and/or external law enforcement and intelligence agencies determine *the threat is known, but is not verified*.	Medium
The likelihood of a threat, weapon, and tactic being used in the region or against the site or building is negligible. Internal decision makers and/or external law enforcement and intelligence agencies determine the threat is non-existent or extremely unlikely.	Low

Human Caused Threat Rating Results

Human Caused Threat	Rating
Aircraft Accident	Low
Biological Attack	Low
Chemical Agent/Toxic Inhalation Release	Low
Civil Disorder	Low
Conventional Attack	Low
Major Crime	Medium
Cyber Attack	Medium
Mass Shootings/Hostile Event	Medium
IED	Low
Nuclear Attack/Acts of War	Low
Radiological Dispersion Device	Low
Radiological Launch Event	Medium
Sabotage/Theft	Medium
Terrorism	Low
Workplace Violence	Medium

Threats and Hazards of Most Concern

Threats and Hazards of Most Concern		
Natural	Technological	Intentional (Human Caused)
Tropical Storm/Hurricane	Cyber Attack	Cyber Attack
Flooding	Hazardous Materials and Nuclear Incidents	Radiological Launch Event
Severe Storm/Tornado	Radiological Launch Event	Mass Shooting/Hostile Event
	Rail Accident	Major Crime
		Workplace Violence
		Sabotage/Theft

Hazard Profiles

This section contains profiles detailing the characteristics of the hazards of most concern.

Non-Natural Hazard Profile Structure

Technological and human caused threats and hazards require a different approach to evaluating likelihood and potential impacts as compared to natural hazards. With natural hazards, as done in the local hazard mitigation planning process, an evaluation is based on past occurrences, weather patterns, geography, and other relevant earth science. Technological and human caused threats and hazards are not dependent upon earth science and do not occur with regular patterns. For that reason, a modified approach is appropriate for evaluating the potential of technological and human caused threats and hazards.

Each technological or human caused hazard profile contains the following components:

Application Mode: describing the human act(s) or unintended event(s) necessary to cause the hazard to occur.

Duration: the anticipated length of time the hazard is present on the target. For example, the duration of an earthquake may be just seconds, but a chemical warfare agent such as mustard gas, if un-remediated, can persist for days or weeks under the right conditions.

Dynamic/Static Characteristic: describing the hazard's tendency, or that of its effects, to either expand, contract, or remain confined in time, magnitude, and space. For example, the physical destruction caused by an earthquake is generally confined to the place in which it occurs, and it does not usually get worse unless there are aftershocks or other cascading failures; in contrast, a cloud of chlorine gas leaking from a storage tank can change location by drifting with the wind and can diminish in danger by dissipating over time.

Mitigating Conditions: characteristics of the target and its physical environment that can reduce the effects of a hazard. For example, earthen berms can provide protection from bombs; exposure to sunlight can render some biological agents ineffective; and effective perimeter lighting and surveillance can minimize the likelihood of someone approaching a target unseen.

Exacerbating Conditions: characteristics that can enhance or magnify the effects of a hazard. For example, depressions or low areas in terrain can trap heavy vapors, and proliferation of street furniture (trash receptacles, newspaper vending machines, mail boxes, etc.) can provide concealment opportunities for explosive devises.

Hazardous Waste/Materials Spill Profile

Hazardous waste/materials are widely used or created at facilities such as hospitals, wastewater treatment plants, universities and industrial/manufacturing warehouses. Several household products such as cleaning supplies and paint are also considered hazardous materials and can be found in households and stores. Hazardous materials include:

- Explosives;
- Flammable, non-flammable, and poison gas;
- Flammable liquids;
- Flammable, spontaneously combustible, and dangerous when wet solids;
- Oxidizers and organic peroxides;
- Poisons and infectious substances;
- Radioactive materials; and
- Corrosive materials.

The release of a hazardous material to the environment could cause a multitude of problems. Although these incidents can happen almost anywhere, certain areas of the City are at higher risk, such as near roadways that are frequently used for transporting hazardous materials and locations with industrial facilities that use, store, or dispose of such materials. Areas crossed by railways, waterways, airways, and pipelines also have increased potential for mishaps. Incidences can occur during production, storage, transportation, use, or disposal of hazardous materials. Communities can be at risk if a chemical is used unsafely or released in harmful amounts into the environment. Hazardous materials can cause death, serious injury, long-lasting health effects, and damage to buildings, the environment, homes, and other property.

Application mode: Hazardous waste/materials spills may be accidental or intentional, and may occur at fixed facilities or on vehicles.

Accidental Hazardous Waste/Materials Spill

Hazardous materials accidents can range from a chemical spill on a highway to groundwater contamination by naturally occurring methane gas to a household hazardous materials accident. Potential hazards can occur during any stage of use from production and storage to transportation, use or disposal. Production and storage occur in chemical plants, gas stations, hospitals, and many other sites. There are many reasons an unintentional hazardous waste/materials spill may occur. Some of these include:

- Malfunction of equipment
- Natural disaster

- Accidents caused by humans

Intentional Fixed Facility Hazardous Waste/Materials Spill

Hazardous material spills at fixed facilities may be internal or external to the facility. External releases may involve industrial storage, fires, or malicious acts. External releases may create airborne plumes of chemical, biological, or radiological elements that can affect a wide area and last for hours or days. Internal releases occur inside buildings and can be caused by a chemical spill or release of a biological or radiological agent. Internal releases can affect all occupants of a building, particularly if the material is distributed throughout the building through the heating/ventilation system.

Intentional hazardous material releases at fixed facilities might include:

- Deliberate release of a hazardous substance by an employee of a facility that stores or uses hazardous materials or produces hazardous waste;
- Deliberate release of a hazardous substance into the water supply
- Detonation of a “dirty bomb” – an explosive device containing radiological or biological substances that are released into the air upon explosion;
- Redirection of toxic waste into water supply or ventilation system; and
- Delivery or placement of a hazardous material inside a building.

Intentional Mobile Hazardous Waste/Materials Spill

Intentional mobile releases may include:

- Release of a chemical, biological, or radiological agent from a moving vehicle or train;
- Use of a vehicle as a dirty bomb, i.e. crashing a vehicle filled with hazardous materials into a structure or building or exploding the vehicle;
- Targeting commercial/industrial chemical containers transported in bulk by both road and rail;
- Release of hazardous materials from airplanes over densely populated areas; and
- Release of hazardous materials into water from a boat.

Duration: Accidental hazardous waste/materials spills can be reported immediately following the spill, thus reducing the amount of time the spill is left uncontained. Most hazardous waste/materials spills occur with little or no warning, and can be difficult to detect until symptoms present themselves to those affected. External releases may create airborne plumes of chemical, biological, or radiological elements that can affect a wide area and last for hours or days. Internal releases will most likely require evacuation of a facility for hours to days. Both external and internal releases require extensive clean-up efforts, lasting from days to months depending on the type and magnitude of the spill.

Dynamic/static characteristics: Both mobile and external hazardous materials releases can spread and affect a wide area, through the release of plumes of chemical, biological or radiological elements, or leaks, or spills. Conversely, internal releases are more likely to be confined to the structure the material is stored in.

Chemicals may be corrosive or otherwise damaging over time. A hazardous materials release could also result in fire or explosion. Contamination may be carried out of the incident area by people, vehicles, wind, and water.

Hazardous material releases are dynamic and may vary depending on the following factors:

- Type and amount of agent released;
- Environmental conditions – The micro-meteorological effects of the buildings and terrain can influence the travel of agents;
- Location of release (urban vs. rural, water vs. air); and
- Remediation time, dependent on a locality's or facility's hazardous material release preparedness programs.

Mitigating conditions: Facilities that store hazardous materials are reported to local and federal governments. Security measures at these facilities can be heightened. Many facilities have their own hazardous materials guides and response plans, including transportation companies who transport hazardous materials.

The Brevard County Fire Department maintains Hazardous Materials Business Plans for every business in the County that handles a hazardous material in quantities above the State's reporting threshold. The County inspects and issues annual permits to approximately 500 businesses with annual hazardous materials permits that necessitate monitoring and inspection.

In addition, Brevard county provides safe hazardous waste disposal for residents and small businesses at a specified Household Hazardous Waste (HHW) Station. Their HHW Program educates the public about the safe use, storage, disposal, and alternatives to hazardous products.

Exacerbating conditions: Cocoa has the potential for a variety of incidents involving hazardous materials. There are areas of businesses all over the city of Cocoa that use hazardous materials. The Fire Department keeps information on the materials used in these areas. Accidental releases from any user could occur;

this presents a danger due to the close proximity of some users to neighborhoods, schools, and other sensitive populations. Staff is currently working on enhancements to existing notification plans and systems.

Within the City there is SR 415, FL-472 along with Interstate 4. The city of Cocoa does not have a railroad that may be used to transport hazardous materials. Areas and people within one mile of a highway, railroad, or industrial area are considered potentially at risk from a hazardous materials release.

Although Cocoa does not use wells for its primary drinking water, pollution of the aquifer is also a concern.

Fire Profile

The entire City of Cocoa is at risk to major fires impacting a section of the City or a large complex. The City has 6,395 housing units and 436 businesses. Localized, single-structure fires sometimes occur in Cocoa.

Application mode: Fires can be accidentally caused through human error including cooking accidents, smoking, or unsafe use of woodstoves or space heaters. Malfunctioning electrical equipment is also a major cause of fire in urban areas. Fires originating in the Wildland-Urban Interface (WUI) also pose a threat as they can spread toward more developed areas and cause significant damage to structures, residents, and natural resources. Arson, or the deliberate burning of property, is also a possibility within City limits. Arson attacks may be imposed upon structures, motor vehicles, wildland areas, or other "nonstructural" properties.

Duration: The duration of an urban fire is dependent on weather conditions, the magnitude of the fire, and fire suppression resources. Structural fires could burn for several hours before being fully contained.

Dynamic/static characteristics: Weather conditions (wind and warm, dry temperatures) and the presence of fire fuel can cause fires to spread away from their source.

Mitigating conditions: In the event of a major fire, auto-aid and mutual-aid agreements with Brevard County Fire Rescue will be utilized. The City strives to minimize exposure to wildland and urban fire hazards through rapid emergency response, a sufficient water supply, proactive fire code enforcement, public education programs, and adequate emergency management preparation. The City has three fire stations, covering an average of 4.7 square miles each, and maintains over 721 fire hydrants, covering 100% of the entire city. In urban areas, arsonists may target abandoned buildings. Limiting the number of abandoned buildings or providing security near these buildings may deter arsonists. Both structure and wildland arson data can be analyzed to depict trends in copycat arsonists as well as in weather and fuel conditions. Documenting these trends in a reporting system may assist in mitigating future cases.

Exacerbating conditions: Increasing development in the wildland-urban interface can exacerbate the spread of a wildfire into developed areas, making these areas vulnerable. While planning and mitigation to reduce the risk of fire in Cocoa's area is controlled, there is still potential a fire in this area could impact the City's public safety, cultural and economic activities, and environmental and natural resource management.

Cyber Attack Profile

A cyber terrorist can infiltrate many institutions including banking, medical, education, government, military, and communication and infrastructure systems. The majority of effective malicious cyber-activity has become web-based. Recent trends indicate that hackers are targeting users to steal personal information and moving away from targeting computers by causing system failure.

Application mode: Common types of cyber-attacks are summarized in the table below.

Common Types of Cyber Attacks

Type of Attack	Description
Denial of service	A method of attack from a single source that denies system access to legitimate users by overwhelming the target computer with messages and blocking legitimate traffic. It can prevent a system from being able to exchange data with other systems or use the internet.
Botnet	A collection of compromised machines (bots) under (unified) control of an attacker (botmaster).
Distributed denial of service	A variant of the denial-of-service attack that uses a coordinated attack from a distributed system of computers rather than from a single source. It often makes use of worms to spread to multiple computers that can then attack the target.
Exploit tools	Publicly available and sophisticated tools that intruders of various skill levels can use to determine vulnerabilities and gain entry into targeted systems.
Logic bombs	A form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering event occurs, such as terminating the programmer's employment.
Phishing	The creation and use of e-mails and Web sites—designed to look like those of well-known legitimate businesses, financial institutions, and government agencies—in order to deceive

	Internet users into disclosing their personal data, such as bank and financial account information and passwords. The phishers then take that information and use it for criminal purposes, such as identity theft and fraud.
Sniffer	Synonymous with packet sniffer. A program that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text.
Trojan horse	A computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute.
Virus	A program that infects computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the infected file is loaded into memory, allowing the virus to infect other files. Unlike the computer worm, a virus requires human involvement (usually unwitting) to propagate.
War Dialing	Simple programs that dial consecutive telephone numbers looking for modems.
War Diving	A method of gaining entry into wireless computer networks using a laptop, antennas, and a wireless network adaptor that involves patrolling locations to gain unauthorized access.
Worm	An independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate.

One of the difficulties of malicious cyber activity is that its origin could be virtually anyone, virtually anywhere. Table Common Sources of Cybersecurity Threats summarizes common sources of cybersecurity threats.

Common Sources of Cybersecurity Threats

Type of Attack	Description
Bot-network operators	Bot-network operators are hackers; however, instead of breaking into systems for the challenge or bragging rights, they take over multiple systems in order to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available on underground markets (e.g., purchasing a denial-of-service attack, servers to relay spam or phishing attacks, etc.).
Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, organized crime groups are using spam, phishing, and spyware/malware to commit identity theft and online

	fraud. International corporate spies and organized crime organizations also pose a threat to the United States through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop hacker talent.
Foreign intelligence services	Foreign intelligence services use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that could affect the daily lives of U.S. citizens across the country.
Hackers	Hackers break into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use. According to the Central Intelligence Agency, the large majority of hackers do not have the requisite expertise to threaten difficult targets such as critical U.S. networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage.
Insiders	The disgruntled organization insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes outsourcing vendors as well as employees who accidentally introduce malware into systems.
Phishers	Individuals, or small groups, that execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware/malware to accomplish their objectives.
Spammers	Individuals or organizations that distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations (i.e., denial of service).
Spyware/malware authors	Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware. Several destructive computer viruses and worms have harmed files and hard drives, including the Melissa Macro Virus, the Explore. Zip worm, the CIH (Chernobyl) Virus, Nimda, Code Red, Slammer, and Blaster.

Cyber-Terrorists	Cyber-Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken economies or target businesses, and damage public morale and confidence. Cyber-Terrorists may use phishing schemes or spyware/malware in order to generate funds or gather sensitive information.

Given its location, the City of Cocoa is home to many companies that could be subject to a cyber-attack, including the city itself.

Duration: The duration of a cyber-attack is dependent on the complexity of the attack, how widespread it is, how quickly the attack is detected, and the resources available to aid in restoring the system.

Dynamic/static characteristics: A cyber-attack could be geared toward one organization, one type of infrastructure and/or a specific geographical area. The affected area could range from small to large scale. Cyber-attacks generated toward large corporations can negatively affect the economy. The Congressional Research Service study (2008) found the economic impact of cyber-attacks on businesses has grown to over $226 billion annually. Attacks geared toward critical infrastructure and hospitals can result in the loss of life and the loss of basic needs, such as power and water, to the general public. Cyber-attacks can also lead to the loss of operational capacity.

Mitigating conditions: Cocoa has three levels of security to prevent cyber-attacks:

1. A Symantec anti-virus protection for desktops and laptops;
2. Malware Protection Systems for Web and email systems; and
3. A Fortinet Firewall for the IT Network.

In addition, the City is in the process of deploying a vulnerability management system to better protect the IT network. Access control to buildings, such as ID cards and badges, can help regulate the people who have access to an agency's or corporations' cyber network. Cocoa information technology network locations include access control measures to prevent unauthorized access to these controlled areas.

The City has an Energy Assurance Plan that focuses on minimizing energy interruptions during emergencies. The City does have backup generators and Uninterrupted Power Supplies (UPS) on all critical hard drives and servers.

Exacerbating conditions: Humans are the weakest link in a chain of cyber security. It remains difficult to continuously monitor and manage human/operator vulnerability. However, to address this weakness the City has deployed quarterly newsletter to address cyber security issues, and requires employees to change passwords every 90 days and administrative passwords for critical server access.

Radiological Launch Event

A Major Radiological Source (MRS) is defined as Nuclear Reactors and other devices with a potential for criticality and radioactive materials to be launched which requires presidential nuclear launch approval per "National Security Council/Presidential Directive No. 25," paragraph 9. Examples would include, but not be limited to, Radioisotope Power Systems (RPSs), and Radioisotope Heater Units (RHUs)**.**" The RHU produces electrical power by converting heat from the decay of Plutonium 238 (PUO_2). The design of the RHU is such that they will survive intact and prevent the release of Plutonium for most launch accident scenarios. Worst case scenarios for the possible release of Plutonium involve either an on-pad or low-altitude launch catastrophic event.

Application mode: Since the inception of the Space-X program, there have been two rocket explosions on the launch pads during testing. There have not been any impacts to the City of Cocoa.

Duration: A radiological event typically last for several hours, but the duration can be extended to days.

Dynamic/static characteristics: The radioactive material released from an incident involving an MRS will produce alpha (α) radiation.

Mitigating conditions: Principle risk to population will be from inhalation or ingestion of radiation contaminants (α particles).

Exacerbating conditions: Of primary concern for off-site locations is that of perceived threat to life from a catastrophic event. Prevention of mass panic actions among spectators should be of the highest priority. Prevention and control of large crowds will reduce the number and severity of additional incidents which may divert or overwhelm local emergency services agencies.

Conclusion

The City of Cocoa and its local partners should be commended for the tremendous capabilities currently available to prevent, protect against, mitigate, respond to, and recover from hazards and threats. One invaluable strength of the City's emergency management program is the ongoing coordination with local partners.

Communications technology within the City is fairly robust. Mass notification systems are in place through Brevard County Emergency Management. Responders and emergency managers will use the highest level of communication technology available during/immediately following an incident. Social media will be an asset for receiving information from the public regarding attacks and impacts. Communications and notification systems are both for public safety agencies and the general public. The City of Cocoa has interoperable dispatch system via County of Brevard and several adjacent municipalities. An alternate

Emergency Operations Center (EOC) is identified to enable communication coordination should the primary EOC be compromised. WebEOC enables efficient dissemination of incident management information across local government agencies throughout the operational area.

Opportunities for residents and members of the public to contribute to the County's resiliency are bountiful. The Emergency Services Volunteer program provides supplemental resources to the professional first responders and facilitates means for neighbors to help neighbors (including businesses and other entities). This organization includes several County-sponsored emergency preparedness volunteer programs:

- CERT Program
- Auxiliary Communications Services: ARES/RACES

In addition to these formal opportunities for community members to receive training and assist through specific roles, "see something, say something" campaigns are helpful in maintaining vigilance throughout the City. Public education occurs via Cocoa Emergency Management presence on the web https://www.cocoafl.org/299/Emergency-Management-Division providing emergency preparedness information to the "whole community".

Several policies and organizational processes are in place for the City government to achieve long term resiliency. Examples include the zoning ordinance and building code enforcing safe development. Critical Infrastructure and Key Resources (CIKR) sites are tagged in both the City of Cocoa and Brevard County Computer Aided Dispatch (CAD) systems. Current planning efforts include an update to the Comprehensive Emergency Management Plan, nine department Continuity of Operations Plans, and this THIRA report. Establishing a THIRA Executive Committee may prove to be helpful in ongoing planning efforts beyond regular updates of this report.

Much of the City's resiliency and preparedness relies on actions taken by non-City agencies. For example, schools are trained to handle active shooter situations. The Cocoa Beach Regional Chamber of Commerce is a strong resource for coordinating with small businesses.

Despite all of the commendable strengths in emergency management and community resiliency, the THIRA preparation group identified numerous challenges toward further improvement. For example, staff at key institutions and other businesses may not be available following a catastrophic event due to transportation system failure or the need to care for their families. That same problem, of course, may affect City staff.

Resources to respond to a significant event (including first responder professionals, and city staff such as building inspectors) are severely limited. The current contracts and blanket purchase orders are nonexclusive and may result in overlapping needs by multiple jurisdictions/agencies. Following a significant event, personnel resources will be needed for protecting medical supplies, routing traffic safely, etc. Personal preparedness throughout the whole community can be improved.

The THIRA preparation group identified that the business community should be more engaged in emergency/resiliency planning. The local economy is susceptible to impacts from events such as flooding events or cybersecurity attacks.

There is strong concern regarding infrastructure failure throughout the City including power, telecommunications, wastewater distribution, electric distribution, and water distribution to the City's customers.

Other concerns regarding communications following an event include:

- Not all stakeholders have an easy way to report activities.
- Because of social media, the velocity of information, including false information/rumors, is likely to outstrip local governments' ability to stay on top of it.
- Communication systems that public safety relies upon may not be functional.

The City's Office of Emergency Management has limited staffing resources to manage and maintain the desired robust emergency management program. All identified hazards are not fully evaluated in the Local Hazard Mitigation Plan (e.g. Cyber Attack, Hostage/Assassin, Sabotage/Crime/Theft, and Workplace Violence). It requires significant staff time to adequately pre-plan for prevention, protection, mitigation, response and recovery including coordination with numerous local, state, and federal agencies as well as whole community partners.

Recommendations for Action

Throughout the THIRA process, the THIRA preparedness group identified many actions to improve capabilities for prevention, protection, mitigation, response, and recovery. The list below has been modified to summarize clear actionable items the City may prioritize and incorporate into ongoing planning and budgeting processes.

Planning

- Create the City of Cocoa Emergency Operations Plan and incorporate the identified hazards as evaluated in this THIRA.

- Develop a detailed inventory of Critical Infrastructure and Key Resources (CIKR) among Cocoa that will foster improved planning for critical infrastructure protection. Implement a plan to document risks to specified CIKR and develop a strategy to mitigate these risks. This plan could include a template for CIKR managers to conduct and document risk assessments for submission to the City of Cocoa.

Promote Utilities Infrastructure improvements that mitigate/improve resiliency (power, water, wastewater, gas).

- Continue to collaborate with regional planning efforts to mitigate impacts of sea level rise / climate change.
- Implement an Infrastructure Management System.
- Conduct an updated assessment on the vulnerabilities of public safety communication technologies and capabilities.
    - Develop alternate communications capabilities to reduce reliance on commercial carriers.
    - Continue to implement a city-wide public safety communications infrastructure assessment and survey to provide a baseline capability to connect key facilities and nodes.
- Develop an emergency information technology plan, including business continuity and disaster recovery (BCDR).
- Encourage owners of CIKR to develop all hazard response plans and coordinate, where applicable, support requirements with appropriate service providers.
- Develop a City of Cocoa recovery plan including:
    - pre-identified locations for Florida Division of Emergency Management and FEMA trailers and field hospital/medical treatment areas.
    - plans for restoring basic health and social services functions following a catastrophic event pre-identified alternative housing solutions for use following a catastrophic event.
    - an evaluation of options for expediting building permits following a catastrophic event.
- Convene a THIRA executive committee annually to review and update the THIRA.

Organization

Continue to outsource an agency to develop, manage, and coordinate the implementation of the Cocoa family of emergency plans (CEMP, COOP, HMP, THIRA, etc.).

- Use the *Threat and Hazard Identification and Risk Assessment* (THIRA) report to help guide decisions related to prevention, protection, mitigation, response and recovery related to threats that could affect the City.
- Implement a Joint Information System with Brevard County stakeholders that will improve public messaging during times of crises. Maintain trained staff to serve as local alerting authorities consistent with the Integrated Public Alert and Warning system (IPAWS).
- Perform a feasibility study to re-establish our Cocoa Emergency Services Volunteer programs, Community Emergency Response Teams, and similar programs throughout the community.
- Maintain participation in regional efforts to address remaining flood concerns.
- Continue a Multi-Agency Coordination (MAC) structure for storms/floods, public works mutual aid, etc. Evaluate and improve coordination protocols within the Operational Area, and with appropriate state and federal agencies.
- Continue participation in the Central Florida Intelligence Exchange (CFIX), the Intelligence Liaison Officer (ILO) program, and other means to share information among agencies, businesses, and partner organizations.
- Maintain the emergency resource directory and put in place advanced contracts for key commodities or services identified during the planning, training, and exercise process.

Equipment/Facilities

- Develop an Emergency Operations Staging Area (EOSA) to serve as a staging area resource and to shelter critical supplies.
- Increase access controls / physical security at critical city owned and operated facilities.
- Maintain at a high level of readiness emergency response vehicles and specialized equipment required to respond to the threats and hazards listed in this report.
- Acquire alternative energy and energy efficient equipment that will reduce fuel requirements and ease overall logistical burdens.
- Upgrade stormwater monitoring systems to provide improved situational awareness during storm events.
- Coordinate with appropriate organizations to install battery backup systems on traffic signals that increase public safety following a power outage scenario.
- Improve connectivity to partner EOCs and 911 PSAPs such as fiber, microwave, etc.
- Explore Video Teleconferencing (VTC) capabilities to link government and nongovernment partners.

- Upgrade command and control software systems that improve communications, collaboration, and situational awareness.
- Acquire base camp supplies and materials to sustain small response operations (30-50 responders) for events that occur in or around Cocoa.
- Continue to participate in CBRNE and HAZMAT equipment evaluation and selection.
- Continue to evaluate feasibility of alternate facilities.

Training and Exercise

- Collaborate and regularly exercise with agencies/organizations referenced in the City's Emergency Operations Plan: Federal, State, agencies with a regional presence; Mutual Aid Jurisdictions, Schools and Universities, Private Sector businesses, Not for Profit organizations (Faith Based, Community Service); Hospitals & Health Care Facilities.
    - Conduct training with other government agencies to ensure collaborative processes and work through specific scenario variables.
    - Participate in collaborative planning, training and exercises with Sunrail and CSX operating in the area.
    - Train and exercise road block/traffic diversion procedures.
- Conduct training and exercises with private sector entities such as Shopping Center, etc.
- Regularly conduct ICS and EOC staff training per the Cocoa EOC Staff Development Program prioritizing high threat hazards
- Conduct employee information technology security and awareness training and exercise a cyber security response effort with the information technology department as the operations lead.

Community Readiness

• Cultivate a culture of preparedness and community connection through efforts such as outreach to public and private schools, Citizen Corps Council, City Staff and Volunteer Disaster Service Worker training, and other "whole community" stakeholders.

o Continue to engage the business sector to improve their mitigation and preparedness efforts; educate small businesses on the importance of resiliency planning.

o Establish a goal for each family and business within the community to have an adequate supply of water, food, etc.

o Pre-identify/establish public messaging campaigns that remind the community of appropriate actions to a variety of potential hazard events (e.g. shelter in place, evacuate, hurricanes, flooding, etc.)

o Continue and improve promotion of family and business readiness to mitigate service needs such as sheltering and mass care.

THIRA Maintenance

The City of Cocoa Fire Department Emergency Management will be responsible for reviewing this THIRA report to make note of progress and/or items to update. Annually, the THIRA Executive Committee will convene to discuss the progress and/or circumstances requiring changes to the stated priorities. The annual Executive Committee meeting will culminate in a summary memo prepared by Emergency Management.

Every two years the THIRA report will be updated and re-issued as a new version. On an ongoing basis the THIRA report shall inform updates to the City's Emergency Operations Plan.