CITY OF TYBEE ISLAND

A G E N D A
REGULAR MEETING OF TYBEE ISLAND CITY COUNCIL
January 26, 2023 at 6:30 PM

Please silence all cell phones during Council Meetings

Opening Ceremonies
- Call to Order
- Invocation
- Pledge of Allegiance

Consideration of Items for Consent Agenda

Announcements

Recognitions and Proclamations

1. Chief Tiffany Hayes:
   - Officer Garrett Goatley: Officer of the Year
   - Erin Martinez: Civilian Employee of the Year

Consideration of the approval of the minutes of the meetings of the Tybee island City Council

Reports of Staff, Boards, Standing Committees and/or Invited Guest. Limit reports to 10 minutes.

2. COL Joseph Geary, Commander, Savannah District, Jared M. Lopes, Planning Branch, Savannah District, and Richard Styles, Engineering Research and Development Center, US Army Corps of Engineers: Ship Wake Study Presentation

If there is anyone wishing to speak to anything on the agenda, please come forward. Please limit your comments to 3-5 minutes.

Consideration of Approval of Consent Agenda

Consideration of Bids, Contracts, Agreements and Expenditures

3. Contract for the Public Defender, Jennifer Ozer: Budget Amendment transfer $2750 from General Fund to line item 100-2650-52-1211.
4. Motorola Cyber Security Service

Council, Officials and City Attorney Considerations and Comments

5. Bubba Hughes:
   - Proposed Ordinance: Equitable Distribution FOR DISCUSSION ONLY
   - 708 Butler Avenue
7. Brian West:
   - Wagging Winter Wednesdays
   - Workforce Housing
8. Shawn Gillen: Mid-year update to the Strategic Plan FY 2023

Executive Session

Discuss litigation, personnel and real estate

Possible vote on litigation, personnel and real estate discussed in executive session

Adjournment

Individuals with disabilities who require certain accommodations in order to allow them to observe and/or participate in this meeting, or who have questions regarding the accessibility of the meeting or the facilities are required to contact Jan LeViner at 912.472.5080 promptly to allow the City to make reasonable accommodations for those persons.

*__PLEASE NOTE:__ Citizens wishing to speak on items listed on the agenda, other than public hearings, should do so during the citizens to be heard section. Citizens wishing to place items on the council meeting agenda must submit an agenda request form to the City Clerk's office by Thursday at 5:00PM prior to the next scheduled meeting. Agenda request forms are available outside the Clerk's office at City Hall and at www.cityoftybee.org.

THE VISION OF THE CITY OF TYBEE ISLAND

"is to make Tybee Island the premier beach community in which to live, work, and play."

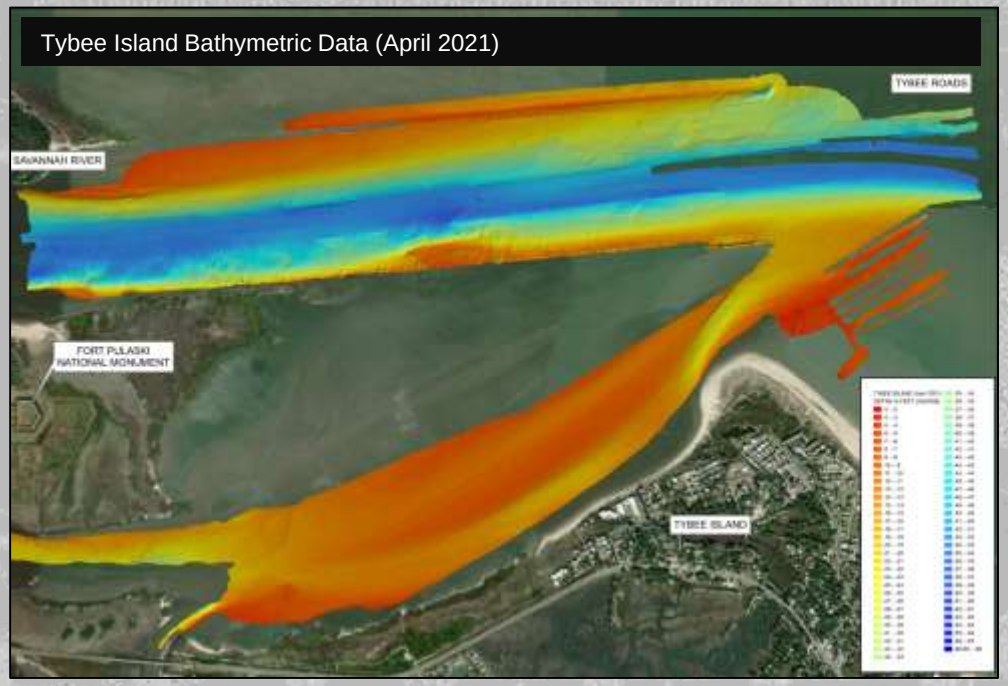
THE MISSION OF THE CITY OF TYBEE ISLAND

"is to provide a safe, secure and sustainable environment by delivering superior services through responsible planning, preservation of our natural and historic resources, and partnership with our community to ensure economic opportunity, a vibrant quality of life, and a thriving future."

File Attachments for Item:

2. COL Joseph Geary, Commander, Savannah District, Jared M. Lopes, Planning Branch, Savannah District, and Richard Styles, Engineering Research and Development Center, US Army Corps of Engineers: Ship Wake Study Presentation

TYBEE ISLAND VESSEL WAKE STUDY - OVERVIEW



U.S. Army Engineer Research and Development Center, Coastal and Hydraulics Laboratory

U.S. Army Corps of Engineers
Savannah District

Date: **26 January 2023**

US Army Corps of Engineers

ERDC

CHL COASTAL & HYDRAULICS LABORATORY

CITY OF TYBEE ISLAND GA
INCORPORATED OCTOBER 15, 1887

TYBEE ISLAND VESSEL WAKE STUDY

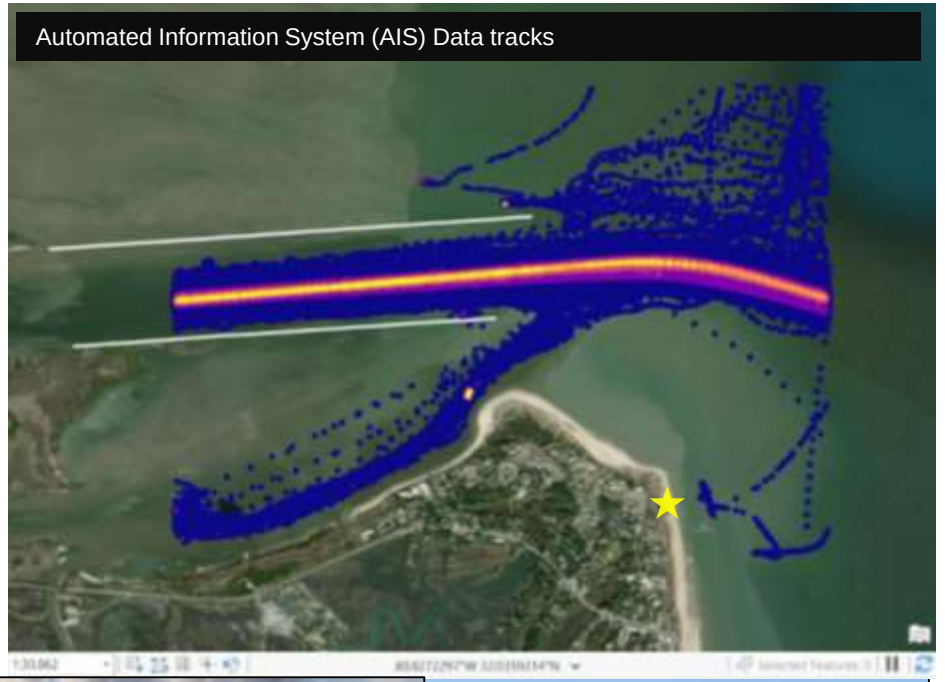
Authority: Section 22 of the Water Resources Development Act of 1974 – Planning Assistance to States (Technical Assistance).

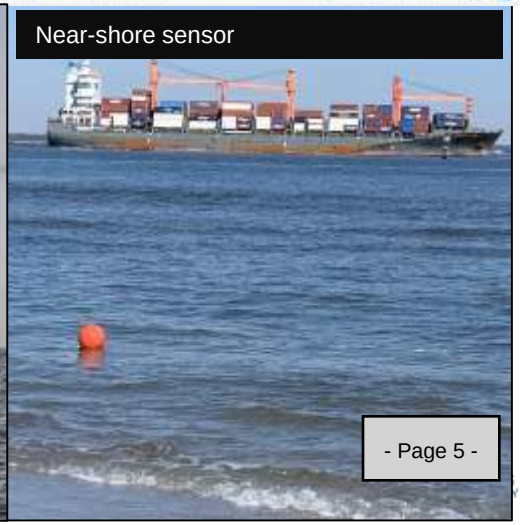
Study Costs: $350,000. Cost-shared (50%) by USACE and the City of Tybee Island.

Problem & Objectives: City of Tybee Island is concerned about the ongoing risk to beachgoers posed by vessel-generated wake on Tybee Island's northern shore. The goal of the study is to develop a better understanding of vessel traffic patterns and associated boat wake generated by large commercial vessels.

Approach: Monitor vessel operations (size, speed, type, heading) and environmental conditions (tides, waves) for a period of approximately 4 months (late July- early December 2021) to better understand the conditions that lead to these large wakes.

Status: The final technical report was published on December 1, 2022. The report can be accessed at: https://erdc-library.erdc.dren.mil/jspui/handle/11681/46140



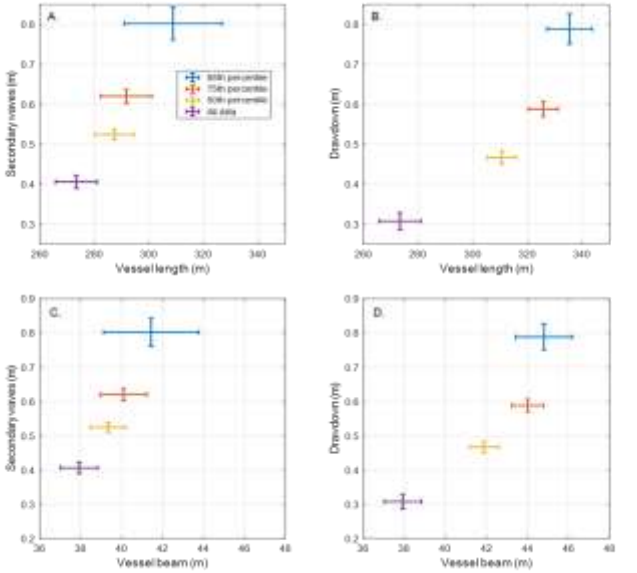


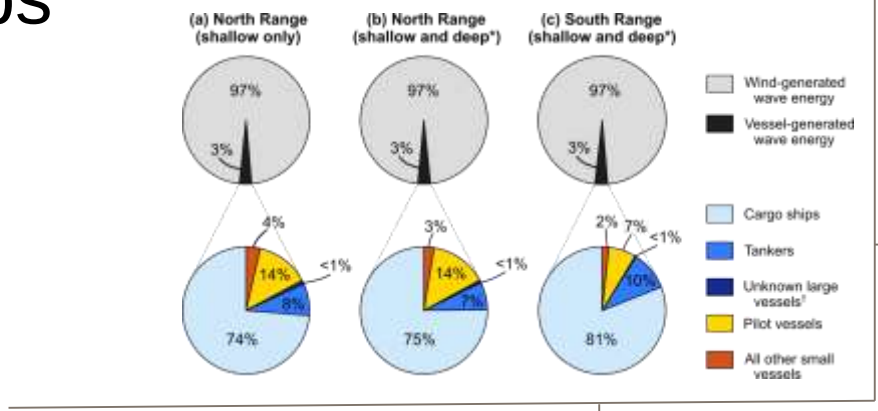
FINDINGS

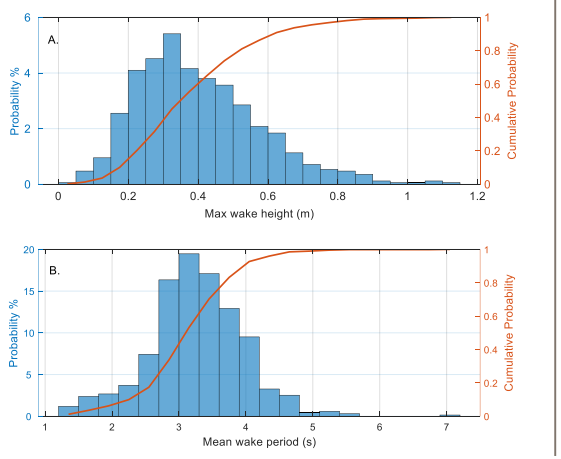
*Data from 1,386 cargo vessel passages and 202 tanker passages

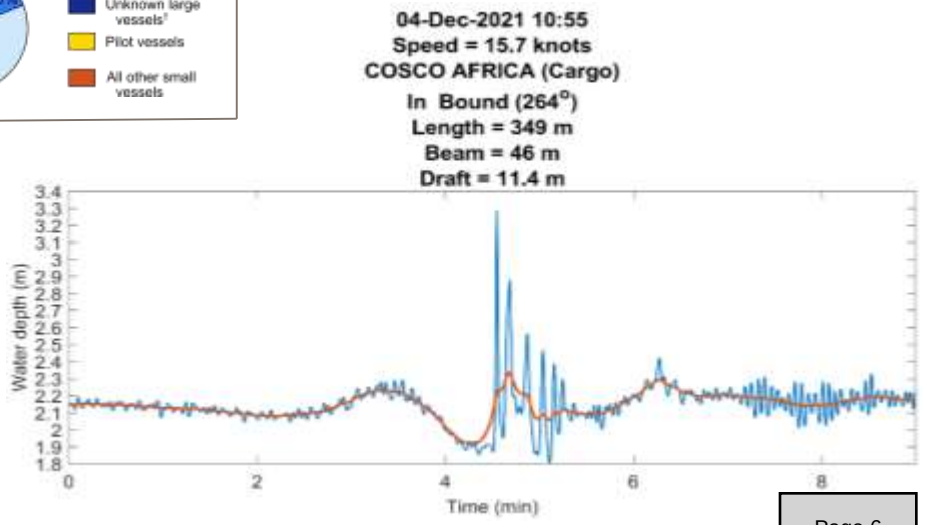
- Largest vessel wake:
  - ✓ Container ships and vehicle carriers
  - ✓ Traveling at higher speeds > 12 knots
  - ✓ Longer and wider ships

- Other influences:
  - ➢ Tidal currents
  - ➢ Wind waves
  - ➢ Vessel direction







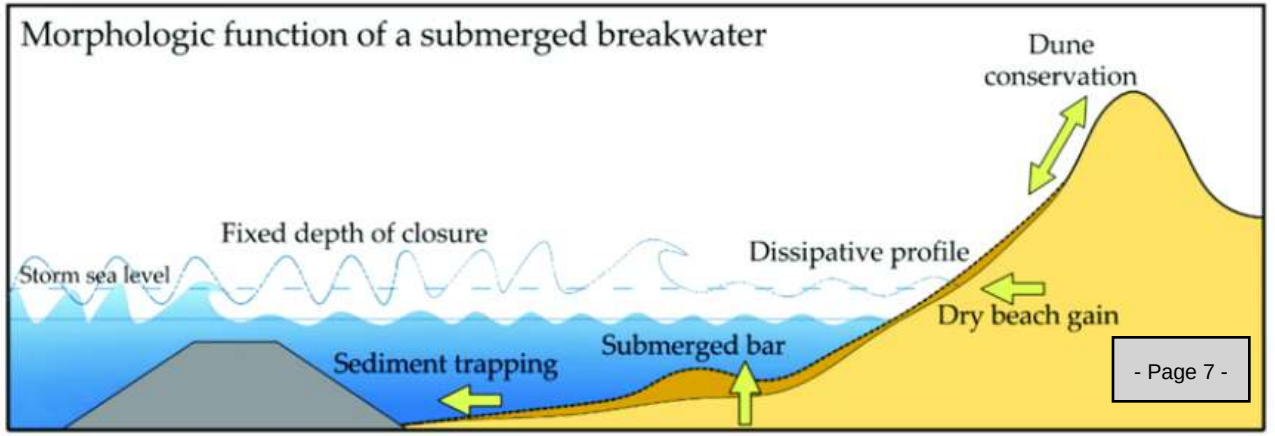


NEXT STEPS

Explore feasibility of breakwater option:

- Measure waves and currents at North Beach to determine appropriate breakwater size and placement
- Model waves, tides and currents to determine if the breakwater affects shoreline erosion
- Model commercial vessels to determine the breakwater design to reduce the impact at the beach

Example) A series of breakwaters promoting sediment accretion at Colonial National Historic Park, Virginia.



File Attachments for Item:

3. -Contract for the Public Defender, Jennifer Ozer: Budget Amendment transfer $2750 from General Fund to line item 745-00-12-1211

AGENDA ITEM

CITY COUNCIL MEETING: January 26

The contract for the public defender, Jennifer Ozer was update and approved by City Council on 12/14/2022. The contract amount increased by $5,550. I am requesting $2750 additional funds to cover until next budget cycle.

Transfer $2750 from General Fund to line item 745-00-12-1211 (Attorneys)

ATTACHMENTS

BUDGET LINE ITEM TRANSFER REQUEST - COURT.pdf

CITY OF TYBEE ISLAND, GEORGIA
BUDGET LINE ITEM TRANSFER REQUEST FORM

Submitted By: Kim Hallstein

Department: Court

Date: 1/4/2023

Purpose: To adjust public defender budget due to increase in annual contract amount approved by City Attorney

Date Received by Finance:

Department	Account Description	Account Number	Current Budget	(Expenditures)	Budget Balance	Requested Budget Adjustment DECREASE	```	Adjusted Budget Balance
LINE ITEM DECREASES								
GF	Fund Balance	100-00-39-1300	0.00	0.00	0.00	2,750.00		(2,750.00)
			0.00	0.00	0.00			0.00
					0.00			0.00
					0.00			0.00
					0.00			0.00
					0.00			0.00
					0.00			0.00
				SUBTOTAL LINE ITEM DECREASES:		**$ 2,750.00**	**xx**	

Department	Account Description	Account Number	Current Budget	(Expenditures)	Budget Balance	```	INCREASE	Budget Balance
LINE ITEM INCREASES								
Court	Attorney (public defenders)	100-2650-52-1211	19,700.00	8,329.13	11,370.87		2,750.00	14,120.87
					0.00			0.00
					0.00			0.00
					0.00			0.00
					0.00			0.00
					0.00			0.00
					0.00			0.00
				SUBTOTAL LINE ITEM INCREASES:		**xx**	**$ 2,750.00**	
					Net Change	**$ 2,750.00**	**$ 2,750.00**	$ -

Signature : Kim Hallstein Date 1/6/2023

Was ...get Amendment Request approved by the City Council? ☐ YES ☐ NO ☐ N/A

If ...ase indicate the date approval was given: _____

At ...by of Agenda Item and minutes from the City Council Meeting

Signature of Finance Employee who Processed the Request: _____

Date: _____

App... _____ Date: _____

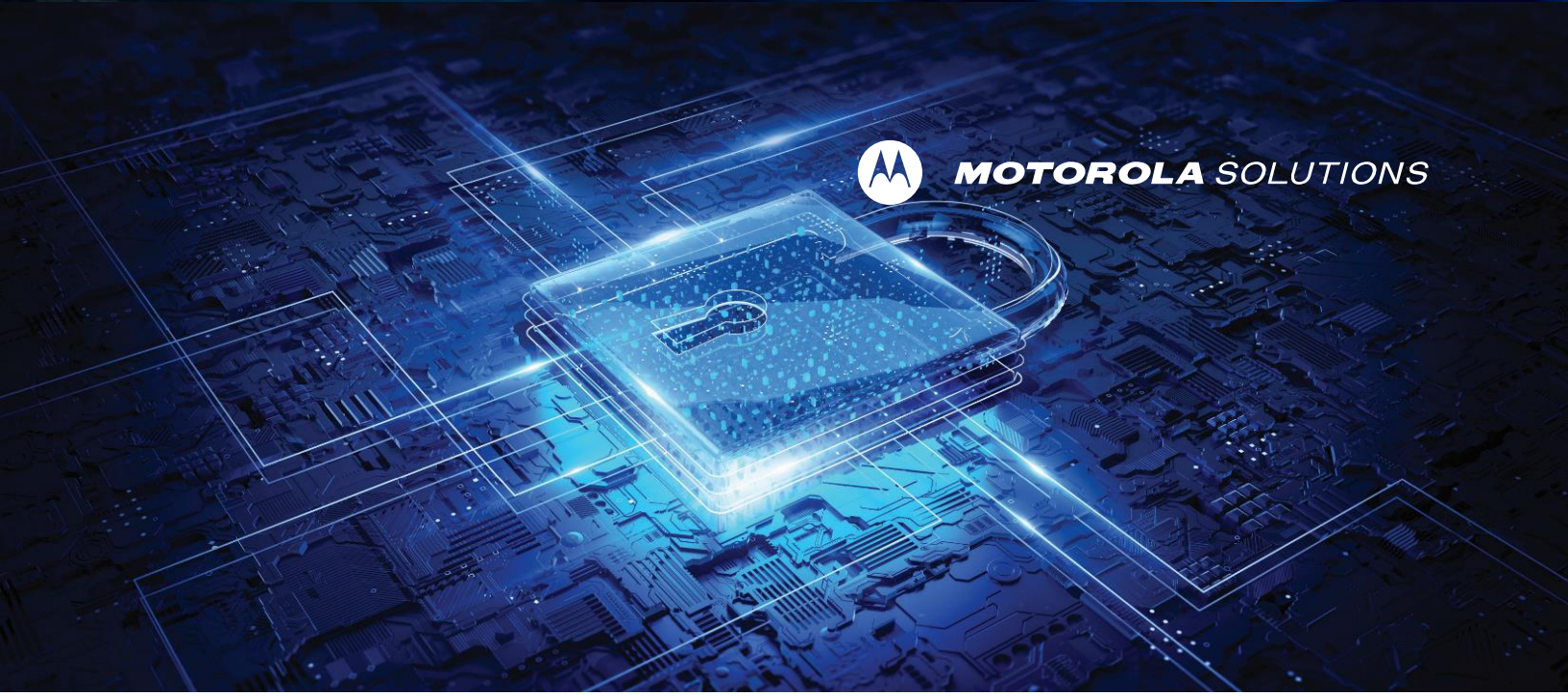
Budget Line Item Transfer Request for Municipal Court

The contract for the public defender, Jennifer Ozer was update and approved by City Council on 12/14/2022. The contract amount increased by $5,550. I am requesting $2750 additional funds to cover until next budget cycle.

K Hallstein 1/6/2023

File Attachments for Item:

4. Motorola Cyber Security Service



Firm Fixed Price Proposal

City of Tybee Island

VESTA Managed Detection and Response

23-145990 / Cybersecurity Services

January 4, 2023

Table of Contents

Motorola Solutions, Inc.
500 W Monroe Street, Ste 4400
Chicago, IL 60661-3781
USA

January 4, 2023

Tiffany Hayes
Chief, Tybee Island Police Department
78 Van Horne Avenue
Tybee Island, GA 31328

RE: VESTA Managed Detection & Response

Dear Chief Hayes,

Motorola Solutions, Inc. (Motorola Solutions) appreciates the opportunity to provide the City of Tybee Island quality cybersecurity equipment and services. Motorola Solutions' project team has taken great care to propose a solution to address your needs and provide exceptional value.

VESTA Managed Detection & Response

Motorola Solution's proposal is conditional upon the City of Tybee Island's acceptance of the terms and conditions included in the executed Communications Systems and Services Agreement. Pricing will remain valid for ninety (90) days from the date of this proposal.

Any questions the City of Tybee Island has regarding this proposal can be directed to Matt Priebe, Cybersecurity Account Manager at 678-206-7756 or by email at matt.priebe@motorolasolutions.com.

Our goal is to provide the City of Tybee Island with the best products and services available in the cybersecurity industry. We thank you for the opportunity to present our proposed solution, and we hope to strengthen our relationship by implementing this project.

Sincerely,

Zack Mahon

Zack Mahon
Area Sales Manager, Cybersecurity – North America

MOTOROLA SOLUTIONS, INC.

Section 1

Executive Summary

Motorola Solutions is a national and global leader in the cybersecurity community with our recent acquisitions of both Delta Risk and Lunarline in 2020. We have evolved into a holistic mission critical technology provider, placing Information Technology (IT) as well as cybersecurity at the forefront of importance to protect our customers against threats to the confidentiality, integrity and availability of their operation.

VESTA Managed Detection and Response

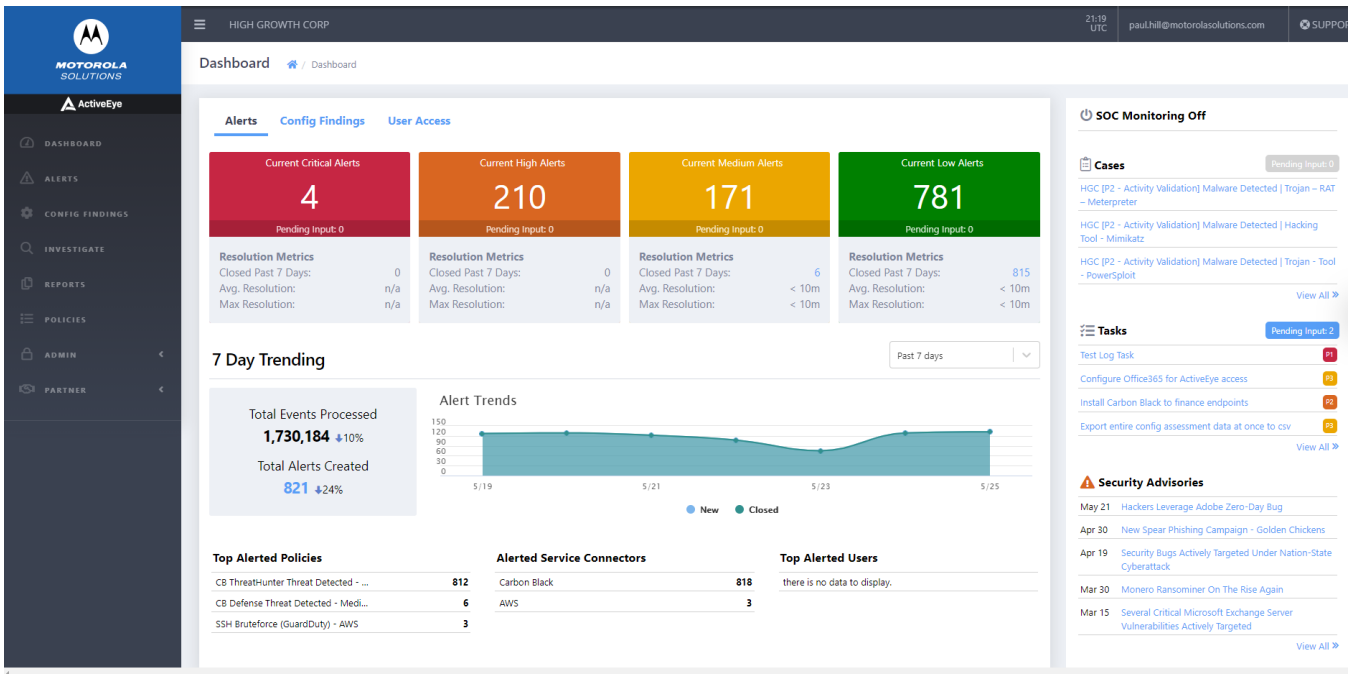
Motorola Solutions VESTA® Managed Detection and Response provides 24/7 monitoring and the expert personnel needed for an effective threat detection solution. As a core feature of this service, the ActiveEye Managed Security Platform continuously collects events from components throughout City of Tybee Island's VESTA 9-1-1 system. ActiveEye applies advanced filtering techniques to remove false positives so that cybersecurity analysts in the Motorola Solutions Security Operations Center (SOC) can review and determine the scope and priority of the remaining alerts to investigate. This is a component of our broader proprietary SOC 2 Type 2 certified Managed Security Platform targeted to Public Safety, Critical Infrastructure, and State/Local municipalities.

The ActiveEye Platform

In 2020, Motorola Solutions acquired Delta Risk, a leading Managed Security Services Provider (MSSP). The acquisition now allows Motorola Solutions to extend the ActiveEye platform to our customers and deliver a co-managed approach to 24/7 security monitoring operations across IT enterprise environments. The benefits of the ActiveEye platform are demonstrated below:

- Included Public Safety Threat Data Feed — Threat reports covering potential attack vectors based on dark web research. Summaries of actual attacks against public safety and state/local municipalities. Indicator data pulled from a large network of deployed public safety sensors and state/local municipality environments.
- Embedded Threat Intelligence — Threat analysts search dark and surface web for intelligence related to attacks against your organization. Identify compromised accounts, phishing attack setups, exposed data, and more specifically related to your organization.
- Integrated Managed Threat Detection & Response — Consolidate SIEM data and direct threat inputs from endpoint security, network sensors, and cloud/SaaS applications. Pre-built custom playbooks to process alerts and reduce/eliminate manual analyst effort.
- Single Dashboard for Threat Visibility — Prioritize based on actual assets in the environment. Asset inventory created manually or automatically with Managed Vulnerability Assessment Service - external and authenticated scans of assets and provides a complete attack surface map

The ActiveEye platform dashboard can be seen below:



Benefits for the Chief Information Security Officer (CISO)

- Main dashboard displays and aggregates all of the important and relevant risk information from across the organization, helping decision makers to make better, informed decisions to balance cybersecurity efforts and operational efficiencies
- Main dashboard provides key performance metrics and indicators that can inform an admin at a glance to the activity that is occurring throughout their environment.
- Create customize ad-hoc reports and notifications for specific areas of interested to a team.
- Complete transparency into the service that Motorola Solutions is providing. The dashboard will provide the key indicators to the number of events that are handled on a daily, weekly, monthly basis and to how those events are handled by the Motorola SOC.

Public Safety Threat Alliance

Cyber threats to public safety agencies are increasing in scope, scale, and complexity; however, most agencies lack the cybersecurity capabilities required to mitigate risk and ensure continuity of public safety operations. To address this critical need, Motorola Solutions has established a cyber threat information sharing and analysis organization (ISAO) for public safety called The Public Safety Threat Alliance (PSTA). The PSTA is recognized by the U.S. Cybersecurity and Infrastructure Security Association (CISA), and highlights Motorola Solutions' commitment to public safety agencies and the communities they serve.

The PSTA will leverage cybersecurity risk information from across Motorola Solutions' Cybersecurity Services. This, paired with information from members and trusted partners including CISA, other ISAOs, and nonprofits dedicated to sharing cyber threat intelligence, will help generate actionable intelligence to improve members' cybersecurity posture, defense, and resilience against evolving threats to their public safety missions. Membership in the PSTA is open to all public safety agencies. While initial efforts are focused on U.S. public safety, the Alliance will include global public safety

agencies in the future.

Learn more about the Public Safety Threat Alliance at: https://motorolasolutions.com/public-safety-threat-alliance

WHY MOTOROLA SOLUTIONS

Company Background and History

Motorola Solutions creates innovative, mission-critical communication solutions and services that help public safety and commercial customers build safer cities and thriving communities. You can find our products at work in a variety of industries including law enforcement, fire, emergency medical services, national government security, utilities, mining, energy, manufacturing, hospitality, retail, transportation and logistics, education, and public services. Our communication solutions span infrastructure, devices, services and software to help our public safety and commercial customers be more effective and more efficient.

Company Overview

Since 1928, Motorola Solutions, Inc. (formerly Motorola, Inc.) has been committed to innovation in communications and electronics. Our company has achieved many milestones in its history. We pioneered mobile communications in the 1930s with car radios and public safety networks. We made the equipment that carried the first words from the moon in 1969. We commercialized the first handheld portable scanner in 1980. Today, as a global industry leader, excellence in innovation continues to shape the future of the Motorola Solutions brand.

We help people be their best in the moments that matter.

Motorola Solutions connects people through technology. Public safety and commercial customers around the world turn to Motorola Solutions innovations when they want highly connected teams that have the information they need throughout their workdays and in the moments that matter most to them.

Our customers rely on us for the expertise, services and solutions we provide, trusting our years of invention and innovation experience. By partnering with customers and observing how our products can help in their specific industries, we are able to enhance our customers' experience every day.

Motorola Solutions' Corporate Headquarters is located at 500 West Monroe Street, Chicago, IL 60661. Telephone is +1 847.576.5000, and the website is www.motorolasolutions.com.

Section 2

Solution Description

2.1 Solution Overview

Motorola Solutions ("Motorola") is pleased to present the proposed cybersecurity services for the City of Tybee Island (hereinafter referred to as "Customer").

The following cybersecurity services are included in our proposal:

- **VESTA Managed Detection and Response**
  - ActiveEye Remote Security Sensor
  - Log Analytics
  - Intrusion Detection System
- **Motorola Network and Security Operations Center (NSOC) Monitoring and Support**

2.2 Services Included

The ActiveEye service modules included in our proposal are selected in the **Subscribed** column below. The services are based on the following deployment type:

Site Information	
Number of System Deployments	1
Type of System Deployment	Single Site Centralized
Number of Seats	4

Table 2-1. Service Modules

Service Module	Features Included	Subscribed
ActiveEye Remote Security Sensor (AERSS)	Number of sensors: 1 (1) VESTA Managed Detection and Response	X
Log Analytics	Standard features described in Section 2.3.1.	X
Intrusion Detection System	1Gbps monitored across all sensors	X

The Cybersecurity Monitoring services included in our proposal are selected in the **Subscribed** column below.

Table 2-2. Cybersecurity Monitoring

Cybersecurity Monitoring	
Motorola Network and Security Operations Center (NSOC) 24x7	X

2.3 Service Description

VESTA Managed Detection and Response reduces the risk that a cybersecurity threat will impact system availability, integrity, and confidentiality. Qualified cybersecurity analysts with extensive experience working on VESTA 9-1-1 mission-critical systems will monitor the Customer's system for signs of cybersecurity threats.

The VESTA Managed Detection and Response service is performed by Motorola's Network and Security Operations Center (NSOC) using specialized monitoring elements. The NSOC's expert cybersecurity analysts monitor for alerts 24x7x365. If an event that may represent a threat is detected, analysts will investigate and initiate an appropriate Customer engagement. Customer engagements may include, but are not limited to, requesting additional information from the Customer, continuing to monitor the event for further development, or informing the Customer to enact the Customer's documented Incident Response plan.

NSOC analysts rely on monitoring elements to detect signs of a potential threat impacting the Customer's VESTA 9-1-1 system. The following subsections describes these elements.

2.3.1 ActiveEye Security Management

Motorola's ActiveEye Security Management platform collects and analyzes security event streams from ActiveEye Remote Security Sensors in the Customer's VESTA 9-1-1 system, using security orchestration and advanced analytics to identify the most important security events from applicable systems.

The platform automates manual investigation tasks, verifies activity with external threat intelligence sources, and learns what events will require rapid response action. The goal is to reduce time to resolution and contain any security event.

The Customer will receive access to the ActiveEye platform as part of this service. ActiveEye will serve as a single interface to display system security information. Using ActiveEye, the Customer will be able to configure alerts and notifications, review security data, and perform security investigations.

ActiveEye Remote Security Sensor

One or more ActiveEye Remote Security Sensors (AERSS) will be deployed into the VESTA 9-1-1 system to deliver the service. These sensors monitor geo diverse sites in the system for security events and pass security information to the ActiveEye platform.

AERSS integrate the ActiveEye platform with network elements, enabling it to collect logs from Syslog, as well as to analyze network traffic over port(s) and scan elements for vulnerabilities.

The following are the environmental requirements and specifications the Customer must provide to prepare for the AERSS deployment.

Specifications	Requirements
Power Consumption (Max)	550 Watts (Redundant Power Supply)
Power Input	100-240V AC
Current	3.7 A – 7.4 A
Circuit Breaker	Qty. 2
Line Cord	NEMA 5-15P
Heat Disspitation (max)	2107 BTU/hr
Internet Service Bandwidth	Bandwidth throughput 10Mbps

Log Collection / Analytics

The AERSS deployed in the system collect logs and other security information from applicable servers, workstations, switches, routers, and firewalls. This information is forwarded to the ActiveEye platform, which uses advanced analytics to identify signs of cybersecurity incidents.

Intrusion Detection System

The AERSS deployed in the system include an Intrusion Detection System (IDS) that constantly monitors traffic passing across, into, or out of the VESTA 9-1-1 system. The IDS analyzes traffic for signs of malicious activity in real time, and performs packet level and flow level analysis to enable communications modeling. This information is used to identify anomalous behavior that is not captured by pre-defined traffic signatures, including traffic using encrypted connections. The IDS forwards detected suspicious activity to the NSOC for further analysis.

Service Dependencies

It is mandatory that all VESTA Managed Detection and Response customers also subscribe to the Application Monitoring and Response service for VESTA 9-1-1. In the absence of an active Application Monitoring and Response service for VESTA 9-1-1, the VESTA Managed Detection and Response service cannot be delivered.

Section 3

Statement of Work

In accordance with the terms and conditions of the Agreement, this Statement of Work (SOW), including all of its subsections and attachments, defines the principal activities and responsibilities of all parties for the delivery of Motorola Solutions (“Motorola”) cybersecurity services as presented in this proposal to City of Tybee Island (hereinafter referred to as “Customer”).

3.1 VESTA Managed Detection and Response

Motorola will provide cybersecurity monitoring continuously 24x7x365, and respond to detected events in accordance with Section 3.1.2 Priority Level Definitions and Response Times.

Inclusions

Cybersecurity Monitoring provides Intrusion Detection System monitoring for traffic across the entire on-premises VESTA 9-1-1 system. Only select VESTA 9-1-1 on-premises system components support Log Collection / Analytics.

Motorola Responsibilities

- Provide, maintain, and when necessary replace hardware and software required to monitor VESTA 9-1-1 system elements. This includes the ActiveEye Remote Security Sensors (AERSS) and all software operating on it.
- Coordinate with the Customer to maintain authentication credentials where necessary.
- Coordinate with the Customer on any system changes necessary to integrate the AERSS into the system and establish necessary connectivity.
- Maintain trained and accredited technicians.
- Monitor the Customer's system 24x7x365 for malicious or unusual activity.
- Respond to cybersecurity incidents in the Customer's system in accordance with Section 3.1.2 **Priority Level Definitions and Response Times**.
- Work with the Customer to ensure that all devices within the system that support logging have properly configured Syslog which is forwarding events to the AERSS.

Customer Responsibilities

- VESTA Managed Detection and Response requires a connection from the Customer's system to Motorola's NSOC and to the Internet. Establish connectivity with sufficient bandwidth before service commences.
- Allow Motorola continuous remote access to monitor the system. This includes keeping the connection plugged-in, providing passwords, and working with Motorola to understand and maintain proper privileges.
- Provide continuous utility service to any Motorola equipment installed or used at the Customer's premises to support delivery of this service.
- Provide Customer contact information necessary to complete the Customer Support Plan.
- Provide Motorola-dispatched field service technicians with physical access to service equipment when required.
- Comply with the terms of the applicable license agreements between Customer and the non-Motorola software copyright owners.
- Cooperate with Motorola and perform all acts that are reasonable or necessary to enable Motorola to provide the services described in this SOW.

3.1.1 Cybersecurity Incidents

VESTA Managed Detection and Response excludes services to perform physical containment and/or remediation of confirmed cybersecurity incidents, remote or onsite. The Customer may choose to purchase additional Incident Response professional services to assist in the creation of and/or execution of a Customer's Incident Response Plan.

A "Cybersecurity Incident" is defined as an observable event that Motorola Security Analysts have identified that actually or potentially jeopardizes the confidentiality, integrity, or availability of the system. Examples include ransomware or malicious use of PowerShell.

Motorola Responsibilities

- Upon the identification of a Cybersecurity Incident, notify Customer's documented contact and escalation plan.
- Take documented customer approved actions in an attempt to contain a Cybersecurity Incident to the extent enabled via Motorola Managed technology. Communicate to Customer what additional potential containment actions and incident response resources can be taken across Customer managed IT infrastructure.
- Perform investigation using the VESTA Managed Detection and Response integrated and enabled data sources in an initial attempt to determine the extent of a Cybersecurity Incident.
- Document and share Indicators of Compromise and artifacts discovered during investigation. Motorola will not perform on site data collection or official forensic capture activities on physical devices.
- Reasonably liaise with Customer's Incident Response resources as a result of the Cybersecurity Incident supporting any service provider that is performing incident response and/or remediation related to the Cybersecurity Incident.

Customer Responsibilities

- Maintain one named Point Of Contact (POC) to coordinate regular team discussions and organize data collection and capture across the Customer and Motorola teams.
- If required, contract for Incident Response service provider to perform procedures beyond the scope of the VESTA Managed Detection and Response service such as forensic data capture, additional malware removal, system recovery, ransomware payment negotiation, law enforcement engagement, insurance provider communications, identify patient zero, etc.

3.1.2 Priority Level Definitions and Response Times

Table 2-3. Priority Level Definitions and Response Times

Incident Priority	Incident Definition	Response Times
Critical P1	Security incidents that have caused, or are suspected of causing significant and/or widespread damage to the	Response provided 24 hours, 7 days a week, including US Holidays.

	functionality of or information stored within the system. Efforts to recover from the incident may be significant. Examples: • Malware that is not quarantined by anti-virus • Evidence of communication with suspected malicious actors	
High P2	Security incidents that have localized impact, but have the potential to become more serious if not quickly addressed. Effort to recover from the incident may be moderate to significant. Examples: • Malware that is quarantined by anti-virus • Multiple behaviors observed in the system that are consistent with known attacker techniques	Response provided 24 hours, 7 days a week, including US Holidays.
Medium P3	Security incidents potentially indicative of an attacker performing reconnaissance or initial attempts at accessing the system. Effort to recover from the incident may be low to moderate. Examples include: • Suspected unauthorized attempts to log into user accounts • Suspected unauthorized changes to system configurations (firewalls, user accounts, etc.) • Observed failures of security components	Response provided 8 x 5 on standard business days, which is normally Monday through Friday 8AM to 5PM local time, excluding US Holidays.
Low P4	These are typically informational in nature or are service requests from the Customer. Examples include: • User account creation or deletion • Privilege change for existing accounts	Response provided 8 x 5 on standard business days, which is normally Monday through Friday 8AM to 5PM local time, excluding US Holidays.

3.2 Scope Limitations & Clarifications

Service Limitations

Cybersecurity services are inherently limited and will not guarantee that the Customer's system will be error-free or immune to security breaches as a result of any or all of the services described in this proposal. Motorola does not warrant or guarantee that this service will identify all cybersecurity incidents that occur in the Customer's system. Services and deliverables are limited by, among other things, the evolving and often malicious nature of cyber threats, conduct/attacks, as well as the complexity/disparity and evolving nature of Customer computer system environments, including supply chains, integrated software, services, and devices.

Processing of Customer Data in the United States and/or other Locations

Customer understands and agrees that data obtained, accessed or utilized in the performance of the services may be transmitted to, accessed, monitored, and/or otherwise processed by Motorola in the United States (US) and/or other Motorola operations globally. Customer consents to and authorizes all

such processing and agrees to provide, obtain, or post any necessary approvals, consents, or notices that may be necessary to comply with applicable law.

Customer and Third-Party Information

The Customer understands and agrees that Motorola may obtain, use and/or create and use anonymized, aggregated and/or generalized Customer data, such as data relating to actual and potential security threats and vulnerabilities, for its lawful business purposes, including improving its services and sharing and leveraging such information for the benefit of Customer, other customers, and other interested parties. For purposes of this engagement, so long as not specifically identifying the Customer, Customer Data shall not include, and Motorola shall be free to use, share and leverage security threat intelligence and mitigation data generally, including without limitation, third party threat vectors and IP addresses, file hash information, domain names, malware signatures and information, information obtained from third party sources, indicators of compromise, and tactics, techniques, and procedures used learned or developed in the course of providing services.

Section 4

Proposal Pricing

4.1 Pricing Summary

Motorola pricing is based on the services presented. The addition or deletion of any component(s) may subject the total solution price to modifications.

Description	Price
VESTA Managed Detection and Response includes SOC services – Year 1	$25,000.00
Service Setup Cost (One-time Fee)	$2,149.28
Initial Subscription Period Year 1:	**$27,149.28**

Initial Subscription Period after Year 1:

Description	Price
Initial Subscription Period - Year 2	$25,750.00
Initial Subscription Period - Year 3	$26,522.50
Initial Subscription Period - Year 4	$27,318.18
Initial Subscription Period - Year 5	$28,137.72

4.2 Payment Schedule & Terms

Period of Performance

The initial subscription period of the contract will extend five (5) years from the Commencement Date of Service, defined as the date data is available for analysis, or not later than thirty (30) days after Motorola provides the Customer with necessary hardware or software to connect the first data source.

Term

The Term of the contract begins on the Commencement Date of Service and remains in effect until the expiration of the initial period so specified.

Billing

Upon acceptance of this proposal by the Customer, Motorola will invoice the Customer upon the execution of this proposal for all service fees in advance for the full annual amount according to the Pricing table in Section 4 Proposal Pricing

Pricing SummaryThereafter, Motorola will invoice the Customer annually, in advance for (a) the Services to be performed (as applicable); and (b) any other charges incurred as agreed upon between the parties during the term of the subscription.

Customer will make payments to Motorola within thirty (30) days after receipt of each invoice. Customer will make payments when due in the form of a check, cashier's check, or wire transfer drawn on a United States financial institution.

INFLATION ADJUSTMENT. For multi-year agreements, at the end of the first year of the Agreement and each year thereafter, a CPI percentage change calculation shall be performed using the U.S. Department of Labor, Consumer Price Index, all Items, Unadjusted Urban Areas (CPI-U). Should the annual inflation rate increase greater than 3% during the previous year, Motorola shall have the right to increase all future maintenance prices by the CPI increase amount exceeding 3%. All items, not seasonally adjusted shall be used as the measure of CPI for this price adjustment. Measurement will take place once the annual average for the new year has been posted by the Bureau of Labor Statistics. For purposes of illustration, if in year 5 the CPI reported an increase of 8%, Motorola may increase the Year 6 price by 5% (8%-3% base).

Tax

Unless otherwise noted, this proposal excludes sales tax or other applicable taxes (such as Goods and Services Tax, sales tax, Value Added Tax and other taxes of a similar nature). Any tax the customer is subject to will be added to invoices.

ADVANCED THREAT DETECTION AND RESPONSE FOR ENTERPRISE IT

PROTECT YOUR IT NETWORK, ENDPOINTS AND CLOUD

Organizations are increasingly relying on mobile devices and cloud services, making it difficult for traditional network IT and security teams to keep up. With the frequency and severity of attacks increasing, you need the people, technology, and proven methods to swiftly recognize and respond to threats.

INCREASED VISIBILITY

Motorola Solutions bridges your security gaps through continuous monitoring of enterprise network, endpoint, and cloud activity, backed with 24/7 support from our Security Operation Center (SOC) experts.

Our managed security services prevent small threats from evolving into bigger incidents, and reduce the time required to detect, contain and eradicate problems. We focus on your security so you can focus on your business.

From enterprise network traffic monitoring and control to compliance reporting and tracking, we serve as an extension to your security team through our comprehensive managed services approach.

Our ActiveEye℠ advanced threat detection and response platform enables you to see and correlate activity from your entire enterprise and to interact with our SOC team in real time to resolve threats quickly.

24%

OF ORGANIZATIONS HAVE A TEAM FOR RESPONDING TO SECURITY INCIDENTS WHEN THEY HAPPEN BUT DON'T PERFORM 24/7 MONITORING[1]

SYSTEMATIC APPROACH TO MITIGATE RISKS

DETECT
Proactive event monitoring and automated alerts

ANALYZE
Real-time analysis correlation

INVESTIGATE
Incident investigation and evaluation

RESOLVE
Complex incident resolution

REPORT
Advanced data analytics

KEY FEATURES

Our security team works with your organization to make sure potential threats are detected and are resolved quickly. Armed with the tools you already use, our ActiveEye platform optimizes and scales Managed Detection and Response (MDR) capabilities across your enterprise. It eliminates the noise, allowing you to focus on the tasks that need your attention.

DETECT ENTERPRISE NETWORK THREATS

Get powerful threat detection capabilities across your on-premise enterprise landscape to eliminate security blind spots and mitigate unmanaged shadow IT activities. Meet compliance requirements and detect threats with NIDS, monitoring, log retention, reports, and vulnerability assessments.

SECURE DEVICES AND ENDPOINTS

Protect enterprise laptops, servers, mobile devices and more with threat detection, asset discovery, internal traffic analysis, and log collection. ActiveEye monitors all activity 24/7 and analyzes data in real time to automatically identify threat activity to detect and prevent advanced threats as they happen.

PROTECT SaaS APPLICATIONS

We combine configuration best practices with advanced analytics to give you visibility and control into the tools you use every day to drive your business.

KEEP CLOUD INFRASTRUCTURE SAFE

Gain visibility into your cloud infrastructure to stay productive and keep your cloud safe. Configuration assessments identify risks in your cloud. Activity monitoring alerts you to account compromise or abuse of resources.

SEE THREAT ANALYTICS

Our ActiveEye security monitoring platform learns who and what is attacking your organization, building a threat database that analysts can add to manually as well. Advanced machine learning uses this data while profiling users to detect account takeover or insider threats.

RESOLVE INCIDENTS QUICKLY

ActiveEye puts a simple, intuitive investigation capability at the fingertips of even non-security experts. See all related alerts – both open and closed, along with all administrative activity on user accounts – in a single click.

SEE KPIs AT A GLANCE

For a team to optimize their performance, they need insights on their activities. ActiveEye captures key performance indicators (KPIs) around workload, providing the ability to meet service levels and response actions, thus enabling organizations to see at a glance how threats and resolution times are trending over time.

MOTOROLA SOLUTIONS - YOUR TRUSTED PARTNER

As a leading provider of mission-critical solutions, we understand your mission can only be as secure as your partners enable you to be. Our goal is to provide you with transparency, accountability and security that's built-in from the start.

We believe that our set of highly knowledgeable people with industry certifications, best-in-class organizational policies and procedures and state-of-the-art automation and analytics tools enables us to uniquely deliver enhanced cybersecurity solutions that address your needs today and in the future.

GLOBAL SCALE & EXPERIENCE

300+

SECURITY EXPERTS FOCUSED ON 24/7 MONITORING & RESPONSE

9B

SECURITY EVENTS PROACTIVELY MONITORED EACH DAY

100%

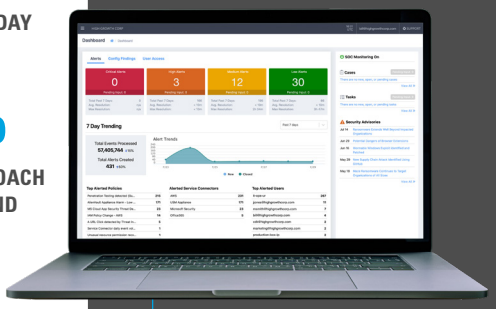
CO-MANAGED APPROACH FOR VISIBILITY AND CONTROL

20+

YEARS OF EXPERIENCE DEVELOPING CYBERSECURITY SOLUTIONS

GET 24/7 CYBERSECURITY COVERAGE

Our ActiveEye advanced threat detection and response platform provides comprehensive, 24/7 cybersecurity coverage, while our SOC experts continuously monitor your systems and data to detect and respond to threats.



Get complete visibility into all security activity via a single view.

For more information on our Advanced Threat Detection and Response Services, contact your Motorola Solutions representative or visit us at **www.motorolasolutions.com/cybersecurity**

Resources

1 Cybersecurity Insiders 2020 State of Managed Security Report

MOTOROLA SOLUTIONS

File Attachments for Item:

5. Bubba Hughes: Proposed Ordinance: Equitable Distribution FOR DISCUSSION ONLY

ORDINANCE NO. 2023-_____

AN ORDINANCE TO AMEND THE CODE OF ORDINANCES RELATING TO ABILITY TO APPLY AND OBTAIN FOR A SHORT-TERM RENTAL PERMIT FOR APPLICANTS HOLDING A BUILDING PERMIT AT THE TIME OF ADOPTION OF THE MORATORIUM AND TO PROVIDE FOR PROCEDURES FOR ADDRESSING REQUESTS FOR SUCH RELIEF AND TO REPEAL CONFLICTING OR INCONSISTENT ORDINANCES AND TO ESTABLISH AN EFFECTIVE DATE

WHEREAS, the duly elected governing authority for the City of Tybee Island, Georgia, is authorized under Article 9, Section 2, Paragraph 3 of the Constitution of the State of Georgia to adopt reasonable ordinances to protect and improve the public health, safety, and welfare of the citizens of Tybee Island, Georgia, and

WHEREAS, the duly elected governing authority for the City of Tybee Island, Georgia, is the Mayor and Council thereof; and

WHEREAS, the governing authority desires to adopt ordinances under its police and home rule powers; and

WHEREAS, Council adopted a moratorium resolution on August 26, 2021 which resolution prohibited the issuance of any new Short-Term Rental ("STR") permits; and

WHEREAS, such resolution was thereafter modified to only apply to properties in R-1, R-1-B and R-2 Zoning Districts; and

WHEREAS, at the time of adoption of the moratorium certain persons had obtained building permits for either new construction or extensive renovations to existing properties which were to be ultimately used as STR properties; and

WHEREAS, these persons who obtained their building permits prior to the moratorium being entered had expectations of being able to obtain an STR permit under the rules and ordinances then in place; however, since the properties were under construction and/or improvements to the extent they were not eligible for certificate of occupancy and therefore unable to apply for a STR permit; and

WHEREAS, an inequitable result could potentially occur if these persons were not permitted to apply for an STR permit and it is the intention of the Mayor and Council to address any such result,

NOW THEREFORE, it is hereby ordained by the governing authority of the City of Tybee Island that the Code of Ordinances will be amended so as to create a new code section so as to provide as follows:

SECTION 1

Certain Building Permit Holders Ability to Obtain STR Permit.

As of the time the moratorium resolution addressing short-term rent adopted on August 26, 2021, any person holding a valid building permit for construction or renovation of a property intended to be used as a STR may apply for an STR permit. Such applicant must establish eligibility for an STR permit under all applicable codes and regulations and must submit their application for an STR permit within six months of the issuance of the Certificate of Occupancy or other official notification that the construction and/or renovations have been completed and passed all applicable required inspections, or within six months of the adoption of this ordinance. In order to be considered for a permit, the applicant must show: 1) the building permit was in place prior to August 26, 2021; 2) the construction and/or renovation was such that no certificate of occupancy for the location could be secured and not certificate of occupancy in fact was not possible due to the renovations; and, 3) the applicant demonstrates by a preponderance of the evidence that the intention was to use the property for a STR by way of records or documents including contracts with agents or Market Place Innkeepers for anticipated rentals intended upon completion of the repairs or construction, or any other evidence the applicant contends supports the intention to establish a STR at the location.

City staff will investigate any such application to determine the existence and nature of the building permit and confirm that such complies with the above requirements to be able to apply for an STR permit.

SECTION 2

If any section, subsection, clause, or provision of this ordinance shall be held to be invalid or unconstitutional by any court of competent jurisdiction, such holding shall not affect any other section, subsection, clause, provision or portion of this ordinance

which is not invalid or unconstitutional. Where the provisions of this ordinance are in conflict with other ordinances, the most restrictive provision shall be enforced.

SECTION 3

All ordinances and parts of ordinances in conflict herewith are expressly repealed.

SECTION 4

This ordinance shall be effective upon its adoption by the Mayor and Council pursuant to the code of the City of Tybee Island, Georgia.

This Ordinance shall become effective on _____ day of _____, 2023.

ADOPTED THIS _____ DAY OF _____, 2023.

_____
MAYOR

ATTEST:

_____
CLERK OF COUNCIL

FIRST READING: _____

572.582 Equitable Consideration 1-4-2023
572.582 Equitable Consideration 10-3-22 REV
572.582 Equitable Considerations 9-29-2022

File Attachments for Item:

7. Brian West:

Wagging Winter Wednesdays

Workforce Housing

REVISED PROPOSAL

Wagging Winter Wednesdays

A Safe, Sanitary, and Wildlife Friendly Proposal for Tybee Island

Many residents on Tybee want to walk their dogs on the beach. In a recent survey, 52% said yes to allowing dogs on the beach.

The Wagging Winter Wednesday proposal was submitted to the City Council meeting on December 10, 2022 for discussion. People for and against the proposal spoke from the floor. Several Council Members voiced their support for a trial period to see how this initiative transpires. Council members also suggested discussions with Code Enforcement and a detail of any costs for the initiative.

The revised beach area at the southern tip of the island from 19th Street to Inlet Ave is proposed. This would allow easy access to the beach by Code Enforcement and participants. Signs (like candidate yard signs) could be placed at 19th Street crossover, Inlet Ave, and on the beach creating a “line in the sand” with an arrow pointing south at 19th St and pointing east at Inlet.

Budget:

30 signs ~$500 Paid by Tybee residents supporting this proposal. Signs would be placed, monitored, and picked up by interested Tybee residents.

Costs for Code Enforcement Officer who could patrol on and off during the day. TBD.

A working diverse group of residents will be formed to oversee this initiative.

Workforce Housing Group Meeting Notes

Jan 6, 2023

Regular attendees: John Bremer, George Calvert, Kelly Calvert, Dustin Church, Amy Gaster, Cody Gay, Spec Hosti, Rev. Sue Jackson, Maria Lancaster, Bob Matkowski, Dillon Patel, Chris Sturgess, Eric Thomas

Advisors: Shawn Gillen, Michelle Ownes

Note: This group was organized by Brian West, Eric Thomas, John Bremer, and Spec Hosti. It is independent and not a part or function of the City of Tybee Island. We seek advice and leadership from City management.

Present this meeting: Shawn Gillen, Michelle Owens, Brian West, Dusty Church, Spec Hosti, Bob Matkowski

Updates from past meetings

Nov 4 Meeting –

- CRC (Coastal Regional Commission) https://www.coastalrc.ga.gov/ –
    - ~$20,000 – Ask City Council to add to 2023-2024 Budget
    - Comprehensive look at housing market and housing needs on Tybee
    - Not a service market analysis – which would advise services needed and how to get services – that would be Main Street / DDA (Downtown Development Authority) function

- Incremental Development Alliance (IDA) https://www.incrementaldevelopment.org/ –
    - Workshops
        - 1 day, beginners
        - 2 day, intermediate
    - small scale process – walks us through plan in small steps
    - Michelle meeting with group Tuesday, Jan 10 via zoom
    - 2 payment models for workshops
        - We host – collect money for attendance
        - They host – collect money for attendance

Current Meeting

- Seek analysis from CRC, then use IDA to help us manage the process.
- Alternative – private firms - $50,000 – 60,000
- Georgia Initiative for Community Housing (GICH) grant https://www.fcs.uga.edu/fhce/gich –
    - opportunity to apply for grant again this year
    - awarded to 5 cities annually –
    - Michelle is leading us through some steps of the process offered by GICH,
        - We must seek funding from other sources
- Do we have potential local developers?
    - Incentives from the City?

- Land Bank – city buys and holds property for development opportunities.
- What can Main St/DDA do?
  - DDA Loans?
  - DDA is able to make purchases and have land banks – can create mechanisms for quick purchases – easier process for DDA, vs. City
  - Their board: Sarah Burnsed chairperson, Kelly Swope, co-chair
    - 3-year term
    - will want a banker, real estate on the board

Action Items

- Brian to provide information on our progress to Council and seek approval for City Attorney to guide in the development of our DDA and Land Bank next steps, place on agenda for the 27th.
- Spec to attend next Main St meeting (Mid Jan.) and seek cooperation from the group.
- Brian and Spec check GMA (Georgia Municipal Association) for classes on DDA process.

Next Meeting – February 3, 2023

- Land Banking primer by Michelle
  - What is Land Banking
  - How does it fit into our Comprehensive Plan?
  - Executive Director of the Savannah Land Bank Authority

File Attachments for Item:

8. Shawn Gillen: Mid-year update to the Strategic Plan FY 2023

AGENDA ITEM

CITY COUNCIL MEETING: January 26

Mid-year update to the strategic plan for the current fiscal year. The City Council created 18 strategic initiatives for the FYE 2023 fiscal year. Staff will report on the progress for each of those initiatives.

Information Only

ATTACHMENTS

Microsoft Word - 2023 Budget - WC.pdf

Letter of Transmittal

Mayor Sessions and the City Council:

Fiscal year 2022 proved to be an exciting year in the City. In the past year, the Island has seen more visitors and more business growth than ever before. Management rose to the challenge of planning the 2023 budget given these ever-changing times. As an organization, we continue to seek out ideas and strategies that will not only maintain, but improve the infrastructure, financial stability and quality of City services while balancing the large fluctuations of visitors to our small island and the goals set by Council. We are committed to looking forward and planning for the future.

The budget for fiscal year 2023 places a greater emphasis on aligning the goals of the City's master plan with the strategic goals developed by the City Mayor and Council. The following strategic goals / focus areas were identified by Council:

> Modify land development code & masterplan

> Prioritize capital projects

> Develop long-term funding plan for City water needs

> Develop plan for improvement of refuse pick-up on beach

> Upgrade park field and playgrounds

> Upgrade landscaping of City owned properties

> Integrate use of solar on new and remodeled buildings

> Create recycling drive-thru facility

> Obtain cost estimates for water treatment & desalination plant

> Increase communication on beach rules

> Increase beach rule enforcement

> Identify other options for room tax revenue

> Increase funding for public safety

> Modify and enhance pension plan

> Develop beach nourishment plan

> Increase street maintenance

> Develop traffic flow and safety improvement plan