# TOWN OF OCEAN BREEZE
# REGULAR TOWN COUNCIL MEETING
# AGENDA

December 9, 2024, 10:30 am
Ocean Breeze Resort Clubhouse Pineapple Bay Room
700 NE Seabreeze Way, Ocean Breeze, FL

***PLEASE TURN OFF CELL PHONES –***
***SPEAK DIRECTLY INTO MICROPHONE***

1. **Call to Order, President Kelley**
   - Pledge of Allegiance
   - Roll Call

2. **Approval of Minutes** – Regular Meeting, Tuesday, November 12, 2024
   (Motion, second, public comment, all in favor)

3. **Mayor Ostrand – Recognition of outgoing Town Council Member Gina Kent**

4. **Swearing-In of Elected Officials, Oath of Office** – Gemma Torcivia, Town Attorney

   Town Council Members:
   - George Ciaschi
   - Janet Galante
   - Sandy Kelley

   Mayor:
   - Karen M. Ostrand

5. **Selection of Council President and Vice President; and Review of Board and Agency Memberships**
   (Motion, second, public comment, all in favor)

6. **Budget to Actual, Fiscal Year Ending September 30, 2024** – Memo from Town Financial Consultant, Holly Vath
   (Motion to accept, second, public comment, all in favor)

7. **RESOLUTION No. 355-2024 – A RESOLUTION OF THE TOWN COUNCIL OF THE TOWN OF OCEAN BREEZE, FLORIDA, TO ADOPT STANDARDS TO SAFEGUARD AGAINST CYBERSECURITY THREATS; ADOPTING THE NIST CYBERSECURITY FRAMEWORK 2.0, PROMULGATED BY THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY; PROVIDING FOR CONFLICTS, SEVERABILITY, AND AN EFFECTIVE DATE**
   (Motion, second, public comment, roll call vote)

8. **Request for a letter supporting Martin County's efforts to secure grant funding to help build a Brightline passenger rail station in Downtown Stuart –** Town Management Consultant, Terry O'Neil
   (Motion, second, public comment, roll call vote)

9. **Comments from the public on topics not on the Agenda**
   **PLEASE LIMIT COMMENTS TO 3 – 5 MINUTES**

10. **Comments from the Council on topics not on the Agenda**

11. **Comments from Town Management Consultant Terry O'Neil**

12. **Comments from Town Attorney Gemma Torcivia**
    - Review of Sunshine Laws and Public Record Laws
    - Update on ADA compliance of Town meeting facility

13. **Comments from Mayor Ostrand**

14. **Announcements** – Regular Town Council Meeting – Monday, January 13, 2024, at 6:00 pm to be held at Ocean Breeze Resort Clubhouse, Pineapple Bay Room, 700 NE Seabreeze Way, Ocean Breeze

15. **Adjourn**
    (Motion, second, all in favor)

Item #2

TOWN OF OCEAN BREEZE
MINUTES REGULAR TOWN COUNCIL MEETING
Tuesday, November 12, 2024, 10:30AM
Ocean Breeze Resort Clubhouse, Pineapple Bay Room
700 NE Seabreeze Way, Ocean Breeze, FL

DRAFT

1. **Call to Order –** Vice President Docherty called the meeting to order at 10:30 a.m.
   - Pledge of Allegiance – Mayor Ostrand led the Pledge of Allegiance
   - Roll Call – Present: Mayor Karen M. Ostrand; Vice President Kevin Docherty; Council Members Gina Kent, Michael Heller, and Matthew Squires; Absent: President Sandy Kelley
   - Staff Present – Town Management Consultant, Terry O'Neil; Attorney, Gemma Torcivia; Permit Processor, Pam Orr; Town Clerk, Kim Stanton

2. **Approval of Minutes –** Council Member Kent, seconded by Council Member Heller, made a motion to accept the Minutes of the following meetings:

- Regular Town Council Meeting, Monday, August 12, 2024
- Regular Town Council Meeting, Monday, September 9, 2024
- Regular Town Council Meeting, Monday, October 14, 2024
- Tentative Budget and Proposed Millage Rate Hearing, Wednesday, September 11, 2024
- Final Budget and Millage Rate Hearing, Wednesday, September 25, 2024

Vice President Docherty asked for comments from the public.

There were none.
(all in favor: Yes: Docherty, Heller, Kent, Squires; No: none; motion passed 4-0)

**3. RESOLUTION No. 356-2024 – A RESOLUTION OF THE TOWN COUNCIL OF THE TOWN OF OCEAN BREEZE, FLORIDA, RATIFYING THE MAYOR'S APPROVAL OF A CONTRACT WITH GIANGRANDE ENGINEERING & PLANNING (GEP) OF STUART, FLORIDA; THEREBY PIGGYBACKING ON GEP'S EXISTING CONTRACT FOR SERVICES WITH THE CITY OF STUART, FLORIDA; PROVIDING FOR AN EFFECTIVE DATE AND FOR OTHER PURPOSES**

Mayor Ostrand explained the need for additional engineering services.

Town Clerk, Kim Stanton, read Resolution No. 356-2024 into the record.

Council Member Kent, seconded by Council Member Squires, made a motion to adopt and approve Resolution No. 356-2024.

Vice President Docherty asked for comments from the public.

Joel Talka, 101 NE Shoal Drive, Ocean Breeze, asked if the terms and conditions of this engagement were commercially relatable, viable and consistent with alternatives.

Attorney Torcivia explained the procurement process of governments in Florida and certain terms within the contract which were tailored to the needs of the Town.

Vice President Docherty asked for further comments from the public.

There were none.
(Roll call vote: Yes: Squires, Heller, Kent, Docherty; No: None; Motion passed 4-0)

**4. Comments from the public on topics not on the agenda** – Vice President Docherty asked for comments from the public on topics not on the Agenda.

There were none.

**5. Comments from the Council on topics not on the agenda** – Vice President Docherty spoke about the new streetlights along Indian River Drive, activities of the Florida League of Cities (FLC) Tax & Finance Committee, FLC webinars and Boys & Girls Clubs of Martin County program called AmeriCorps.

Council Member Heller asked about the status of Martin County's position regarding quiet zones.

Mr. O'Neil answered that the status remained unresolved.

Council Member Kent spoke about the status of Brightline within Martin County.

Vice President Docherty spoke about the status of refurbishing the crosswalks on Indian River Drive.

Council Member Kent spoke about the safety of pedestrians in Jensen Beach.

Vice President Docherty spoke about the representation at the CRA for Jensen Beach.

Vice President Docherty asked for further comments from the Council.

There were none.

**6. Comments from Town Attorney, Gemma Torcivia** – Attorney Torcivia gave an update regarding closeout issues with Ocean Breeze Resort and Seawalk. She stated that negotiations are taking place regarding both communities.

Vice President Docherty asked for questions from the public for the Town Attorney.

There were none.

Vice President Docherty introduced Leo Giangrande, Professional Engineer.

Mr. Giangrande spoke about his willingness to work with the Town and assist with the closeout issues.

**7. Comments from the Town Management Consultant, Terry O'Neil** – Mr. O'Neil spoke about Mr. Giangrande's role in assisting the Town with the closeout issues.

**8. Comments from Mayor Ostrand** – Mayor Ostrand asked about a missing bench and waste receptacle which were removed from along the bioswale area of the Resort.

DRAFT

Mr. O'Neil answered that staff would look at the plan to find out if it was a required feature and inquire of the Resort management to get a schedule for replacement.

Mayor Ostrand spoke about attending the Florida League of Cities (FLC) Municipal Development & Zoning Committee meeting. She stated that the subjects of the Florida Building Codes and Affordable Housing were discussed at the committee meeting. She added that certain bills that would be considered by the Florida Legislature, vacation rentals, advocacy, zoning, FLC lobby, Florida Building Codes, unofficial election results, newly elected officials' workshop, Treasure Coast Regional League of Cities' event and forthcoming information regarding advocacy.

Vice President Docherty discussed the importance of residents' involvement in advocacy and advised about how to be involved in Home Rule. He asked for further comments.

Sue Guccione, 174 NE Portside, Ocean Breeze Resort, asked about updates regarding ADA access points to the Resort clubhouse, ladies' room, amenities, and lift for the community pool. She stated that she pays for the amenities in her monthly rent but does not have access to the amenities.

Mr. O'Neil answered that this issue was on the Town's work list because it came up at last month's meeting. He commented that the Building Official would be looking at the plans and the certifications for compliance. He spoke about the Resort being private property and added that the Town was working on this issue and hopefully by the next meeting the Town would have a report from the Building Official and from Leo Giangrande, PE.

Jane Hale, 205 NE Coastal Drive, Ocean Breeze, stated that she believed that the Town Council would want to make its' meetings accessible to the public.

Discussion ensued regarding ADA compliance, Town Council public meetings, residents' advocacy, and ADA compliance.

Sue Guccione stated that she had contacted Sun Communities and was advised that Sun Communities would not do anything until they heard from the State. She added that she was provided with the information to contact the State and asked why she should have to perform these duties. She asked about entry buttons on the doors and added that she was advised that the Resort was ADA compliant.

Mayor Ostrand explained that this was a process that the Town would have to undertake to ensure that the Resort was ADA compliant.

Discussion ensued regarding public meetings and ADA compliance.

Attorney Torcivia spoke about the range of guidelines regarding ADA compliance. She commented that the Town would investigate the matter and report back to the residents. She added that private citizens had the right to file a complaint and advocate for an optimal solution.

Discussion ensued regarding ADA compliance, public meetings, and accessibility.

George Ciaschi, 261 NE Coastal Drive, Ocean Breeze, stated that the previous management at the Resort told him that he would attempt to provide an engineering report regarding the ADA compliance of the Resort. He commented that he had emailed the previous management and current management, Aaron Smith, with the ADA regulations. He added that he would pursue this issue to get a resolution.

Vice President Docherty stated that the Town would follow-up regarding this issue.

**9. Announcements** – The Regular Town Council meeting to be held on Monday, December 9, 2024, at 10:30 am at the Ocean Breeze Resort Clubhouse, Pineapple Bay Room, 700 NE Seabreeze Way, Ocean Breeze.

Vice President Docherty made the announcement that the official election results would be provided by the Martin County Supervisor of Elections on or before Saturday, November 16th, 2024, and the newly elected officials will be sworn in at the December 9th meeting.

**10. Adjourn –** Council Member Heller, seconded by Council Member Squires, made a Motion to adjourn the meeting at 11:28AM.

Respectfully Submitted,

Kim Stanton
Town Clerk

Minutes approved: ________________________________

DRAFT

Item #4

# TOWN OF OCEAN BREEZE

# OATH OF OFFICE

STATE OF FLORIDA
COUNTY OF MARTIN

"I do solemnly swear (or affirm) that I will support, honor, protect and defend the Constitution and Government of the United States of America and of the State of Florida; that I am duly qualified to hold office under the Constitution of the State and under the Charter of the Town of Ocean Breeze; and that I will faithfully perform the duties of the Town Council to the best of my abilities, so help me God."

______________________________________
George Ciaschi

STATE OF FLORIDA
COUNTY OF MARTIN

Sworn to and subscribed before me this _______ day of ______________________________, _______ A.D., personally appeared before me ______________________________, personally known by me _______ or produced driver's license or passport #______________________________.

______________________________________
Notary

Item #4

# TOWN OF OCEAN BREEZE

## OATH OF OFFICE

STATE OF FLORIDA
COUNTY OF MARTIN

"I do solemnly swear (or affirm) that I will support, honor, protect and defend the Constitution and Government of the United States of America and of the State of Florida; that I am duly qualified to hold office under the Constitution of the State and under the Charter of the Town of Ocean Breeze; and that I will faithfully perform the duties of the Town Council to the best of my abilities, so help me God."

______________________________________
Janet Galante

STATE OF FLORIDA
COUNTY OF MARTIN

Sworn to and subscribed before me this _______ day of ______________________________, _______ A.D., personally appeared before me ______________________________, personally known by me _______ or produced driver's license or passport
#______________________________.

______________________________________
Notary

Item #4

# TOWN OF OCEAN BREEZE

# OATH OF OFFICE

STATE OF FLORIDA
COUNTY OF MARTIN

"I do solemnly swear (or affirm) that I will support, honor, protect and defend the Constitution and Government of the United States of America and of the State of Florida; that I am duly qualified to hold office under the Constitution of the State and under the Charter of the Town of Ocean Breeze; and that I will faithfully perform the duties of the Town Council to the best of my abilities, so help me God."

______________________________________
Sandy Kelley

STATE OF FLORIDA
COUNTY OF MARTIN

Sworn to and subscribed before me this _______ day of ______________________________, _______ A.D., personally appeared before me ______________________________, personally known by me _______ or produced driver's license or passport #______________________________.

______________________________________
Notary

Item#4

# TOWN OF OCEAN BREEZE

# OATH OF OFFICE

STATE OF FLORIDA
COUNTY OF MARTIN

"I do solemnly swear (or affirm) that I will support, honor, protect and defend the Constitution and Government of the United States of America and of the State of Florida; that I am duly qualified to hold office under the Constitution of the State and under the Charter of the Town of Ocean Breeze; and that I will faithfully perform the duties of the Mayor to the best of my abilities, so help me God."

________________________________________
Karen M. Ostrand

STATE OF FLORIDA
COUNTY OF MARTIN

Sworn to and subscribed before me this _______ day of ______________________________,
_______ A.D., personally appeared before me ______________________________, personally known by me _______ or produced driver's license or passport
#_______________________________.

________________________________________
Notary

Item #5

# MEMORANDUM

TO: Town Council and Mayor
FROM: Kim Stanton, Town Clerk
DATE: December 11, 2023
RE: Annual Election of President and Vice President

After "Oath of Office" on your Agenda, you will need to elect a President and Vice President.

## ANNUAL ELECTION OF PRESIDENT AND VICE PRESIDENT

### Election of President:[1]

1. Attorney Crary asks for nominations for the office of President.
2. Attorney Crary asks if there are any other nominations.
3. Attorney Crary asks for a Motion to close the nominations.
4. Upon Motion made and seconded to close the nominations, the Clerk will call the roll to determine if said Motion passes.
5. If there is more than one nomination, the Clerk will call the roll and Council Members will voice their votes per open ballot.

### Election of Vice President:

1. The new President asks for nominations for the office of Vice President
2. The new President asks if there are any other nominations.
3. The new President asks for a Motion to close the nominations.
4. Upon Motion made and seconded to close the nominations, the Clerk will call the roll to determine if said Motion passes.
5. If there is more than one nomination, the Clerk will call the roll and Council Members will voice their votes per open ballot.

[1] **In the absence of a President, the Town attorney will guide the nomination election process.**

Item #5

# MEMORANDUM

TO: MAYOR OSTRAND AND MEMBERS OF THE TOWN COUNCIL

FROM: KIM STANTON, TOWN CLERK

SUBJECT: MAYOR AND TOWN COUNCIL BOARD APPOINTMENTS AND LIAISON ACTIVITIES

DATE: December 9, 2024

Each December, at its regular meeting, the Town Council members approve certain board appointments and liaison activities. Attached you will find the matrix which outlines the meeting dates and times of the organizations along with a brief description of the activities. Vacancies are highlighted in yellow.

Recommendation:

Discuss vacancies and make appointments by Council vote.

Council \ Mayor Board Appointments and Liaison Activities
January 13, 2025 Regular Town Council Meeting

| Organization | | Town's status | Is the Town entitled to official representation on the organization's board? | If yes, who is currently serving? | Have any Town elected officials, not serving as an official representative, been involved with the organization? | If yes, who? | Comments | Action taken at January 13, 2025 Regular Town Council Meeting |
|---|---|---|---|---|---|---|---|---|
| 1 | **Florida League of Cities (FLC)** - The League's mission is to serve the needs of Florida'a cities and promote local self-government by supporting local voices making local choices to protect and enhance Florida's communities. | Paying Member ($632) | Yes, with over 400 members, membership of the FLC Board is determined via a statewide nominating process, elimination ballots, etc. | Mayor Ostrand, Vice President Docherty | No | | Mayor and Town Council members serve as time and travel budgets permit. | |
| 2 | **Florida League of Cities Legislative Committee Sub Group (FLCLCSG)** - Appointments are typically a one-year commitment and involve developing the League's legislative platform detailing priority issues that are most likely to affect daily municipal governance and local decision making during the upcoming legislative session. Policy committee members also help League staff understand the real-world implications of proposed legislation and are asked to serve as advocates throughout the legislative process. | The Town's elected officials are eligible to seek participation by virtue of its FLC membership. | Yes | Mayor Ostrand, Development, Code Compliance and Redevelopment Committee | Yes | Vice President Docherty, Finance and Taxation Committee | The Mayor currently serves on the Development, Code Compliance and Redevelopment Committee; Vice President Docherty serves on the Finance and Taxation Committee | |
| 3 | **Florida League of Mayors (FLM)** - The FLM was created in 2005 for Florida Mayors. Our membership statement is vision, leadership and public service. FLM is a member-driven organization that exists to serve the educational and professional needs of Florida's Mayors. | Paying Member ($350) | Yes, membership on the board is determined through a statewide nominating process. | Mayor Ostrand | No | | Mayor Ostrand currently serves on the board. | |

Council \ Mayor Board Appointments and Liaison Activities
January 13, 2025 Regular Town Council Meeting

| | Organization | Town's status | Is the Town entitled to official representation on the organization's board? | If yes, who is currently serving? | Have any Town elected officials, not serving as an official representative, been involved with the organization? | If yes, who? | Comments | Action taken at January 13, 2025 Regular Town Council Meeting |
|---|---|---|---|---|---|---|---|---|
| 4 | **Treasure Coast Regional League of Cities (TCRLC) -** The Treasure Coast Regional League of Cities promotes communication, collaboration and education among municipalities of Indian River, Martin, Okeechobee and St. Lucie Counties; encourages effective advocacy for home rule to all levels of government; fosters excellence in local self-governance and represents the Treasure Coast with the Florida League of Cities. | Member (no fee) | Yes, as one of the organization's 16 (+/-) members, the Town is entitled to one member and an alternate on the board. | Mayor Ostrand is serving on this Board | Yes | Vice President Docherty was the alternate for 2024 | **Board meetings** are held monthly on the 3rd Wednesday at 10:00AM at Indian River State College (no meetings in June and August). **Membership meetings** are in Nov., Dec., Mar., and May at various locations (TBD); the July meeting is the BBQ in Okeechebee. | |
| 5 | **Treasure Coast Regional League of Cities Advocacy Team (TCRLCAT) -** encourages effective advocacy for home rule to all levels of government; fosters excellence in local self-governance. | Eligible to participate by virtue of its TCRGLC membership | Yes, the team is generally made up of one or two volunteer representatives form each member jurisdiction. It should be noted that Sunshine Law requirements apply if there are two team members from a single jurisdiction. | Mayor Ostrand, Chairman of Advocacy | Yes | Vice President Docherty, Team Member | | |

| | Organization | Town's status | Is the Town entitled to official representation on the organization's board? | If yes, who is currently serving? | Have any Town elected officials, not serving as an official representative, been involved with the organization? | If yes, who? | Comments | Action taken at January 13, 2025 Regular Town Council Meeting |
|---|---|---|---|---|---|---|---|---|
| 6 | **Treasure Coast Council of Local Governments** - A (congenial) organization of local elected officials from County and Municipal governments and School Boards focused primarily on issues of regional impact. | Currently a member ($200 due in January of each year) | Yes. | In 2024 , Vice President Kevin Docherty was appointed to serve as primary and Council Member Kent to serve as alternate | No | N/A | Council needs to appoint a primary and alternate representative. Meetings are held Jan 8 (Marsh Landing in Fellsmere - installation lunch), Feb 5, Mar 5, Apr 9, May 7, Jun 4, July 2 (Okeechobee BBQ), Sept 3, Oct 1, Nov 5, Dec 3. All meetings are held at 10AM, 2300 Virginia Avenue, Conference 3, Fort Pierce, FL 34982 (unless otherwise indicated). | |
| 7 | **Local Legislative Delegation** - The local County Legislative Delegation Meeting holds its annual public hearing in the Fall each year. The delegation hearing is intended to afford local residents and officials an opportunity to request legislation or state funding and express opinions on issues to be considered by the state legislature. The Legislature is scheduled to convene in session on March 4, 2025 in Tallahassee. | Constituent Local Government | N/A | N/A | Mayor Ostrand and Vice President Docherty regularly attends by virtue of Florida League of Cities participation. | | The local delegation includes Senator Gayle Harrell, Representative John Snyder, Representative Toby Overdorf. Mayor and Town Council members attend as needed and at their own initiative. No fixed schedule. | |

| | Organization | Town's status | Is the Town entitled to official representation on the organization's board? | If yes, who is currently serving? | Have any Town elected officials, not serving as an official representative, been involved with the organization? | If yes, who? | Comments | Action taken at January 13, 2025 Regular Town Council Meeting |
|---|---|---|---|---|---|---|---|---|
| 8 | **Martin Metropolitan Planning Organization (MPO) -** Founded in 1993, the Martin MPO is a federally mandated public agency that works to coordinate the improvement of all facets of the transportation network in Martin County. | Not a member | No. | NA | yes | Mayor and Council Members have routinely attended as needed. | Due to its small population, the Town does not have a seat on the MPO. Gaining membership, which requires broad local government support and ultimately the Governor's approval, is challenging and would involve a considerable "campaign" effort on the part of the Town. The MPO regularly meets and meetings are open to the public. Does Council wish to appoint a liaison to attend? The MPO Board meets on Dec 16, Feb 24, Apr 21, May 19 and June 16 in the Martin County Commission Chambers 9:00AM - 11:00AM (2401 SE Monterey Road). Visit their website for further information. | |
| 9 | **Martin Metropolitan Planning Organization Citizen Advisory Committee (CAC) -** The Citizens Advisory Committee (CAC) strives to represent the citizens of Martin County and is responsible for providing continuous public input for the MPO decision-making process. In this capacity, the Committee reviews and comments on transportation planning documents and relevant issues to be brought before the MPO Board. | Currently, no Town citizen is participating | no | no | yes | Former Council President Ann Kagdis was appointed as a county representative by Commissioner Smith. | Meeting are held Feb 5, May 7 & June 4, 2025 @ 9:00AM - 11:00AM (BOCC Commission Chambers); Joint Advisory Committee Meetings (CAC, TAC and BPAC) are held Dec 2 and Apr 7 from 1:30PM - 3:30PM. | Ann Kagdis, Town of Ocean Breeze resident, stated that she remained on the CAC (August, 2024 TC meeting) |

| Organization | Town's status | Is the Town entitled to official representation on the organization's board? | If yes, who is currently serving? | Have any Town elected officials, not serving as an official representative, been involved with the organization? | If yes, who? | Comments | Action taken at January 13, 2025 Regular Town Council Meeting |
|---|---|---|---|---|---|---|---|
| 10 **Martin Metropolitan Planning Organization Technical Advisory Committee (TAC) -** The Technical Advisory Committee (TAC) is a source of wide-ranging professional expertise for the MPO Board and includes representatives from state and local governmental agencies. The Committee is responsible for advising the Board on all technical matters, including transportation plans, studies, and implementation programs. Additional benefits result from the continuous and worthwhile coordination between Committee Members and agencies. | Vacant | Yes | In 2024, Council Member Squires was appointed to serve as the Town liaison; President Kelley was appointed to serve as the alternate to attend TAC meetings. | No | NA | Council needs to appoint a Member and an alternate. The TAC consists of 12 voting members. The meetings are held Feb 3, May 5 & June 2, 2025 at 1:30PM - 3:30PM (4th Floor Workshop Room, Martin County Administrative Center). Joint Advisory Committee Meetings (CAC, TAC and BPAC) are held Dec 2 and Apr 7 from 1:30PM - 3:30PM. | |
| 11 **Martin Metropolitan Planning Organization Bicycle and Pedestrian Advisory Committee (BPAC) -** The Bicycle & Pedestrian Advisory Committee (BPAC) represents the citizens of Martin County on all bicycle and pedestrian-related issues. The Committee is responsible for providing input into the MPO decision-making process, which includes reviewing and commenting on planning documents and identifying relevant issues to be brought before the MPO Board. | No representation at time time | No; Vice Docherty has served in the past | N/A | No | N/A | Does Council wish to seek participation on this Board? If the Council wishes to pursue membership, it will need to approve a designee to be appointment. If yes, the nominee would need fall within the categories of merchant, homeowner's association, a representative from the disabled community or bicycling community. Meetings are held Feb 10, May 12 & June 9 at 2:00PM - 4:00PM (BOCC Commission Chambers). Joint Advisory Committee meetings (CAC, TAC and BPAC) are held Dec 2 and Apr 7 from 1:30PM - 3:30PM. | |

|  | Organization | Town's status | Is the Town entitled to official representation on the organization's board? | If yes, who is currently serving? | Have any Town elected officials, not serving as an official representative, been involved with the organization? | If yes, who? | Comments | Action taken at January 13, 2025 Regular Town Council Meeting |
|---|---|---|---|---|---|---|---|---|
| 12 | **Martin County/Jensen Beach Community Redevelopment Area (CRA) Neighborhood Advisory Committee (NAC)** - The Jensen Beach Neighborhood Advisory Committee (NAC) meets regularly at the Jensen Beach Community Center on Jensen Beach Boulevard and provides advice and recommendations to the Community Redevelopment Agency regarding the implementation of projects adopted within the Jensen Beach CRA Plan. | Not a member | No. | NA | The Mayor and Council Members have, at times, attended meetings particularly regarding matters of the Town. At the August 12, 2024 Town Council meeting, President Kelley volunteered to be the Town's liaison. | President Kelley | Does Council wish to appoint a designated liaison and an alternate to monitor the activities of this Committee? All meetings are on the first Wednesdays at 5:00PM (unless otherwise noted) at the Jensen Beach Community Center, 1912 NE Jensen Beach Boulevard, Jensen Beach in the months of January, March, May, July , September and November, 2025. |  |
| 13 | **Resilient Martin** - A Martin County initiative assisting the residents of Martin County in understanding the future risks of sea-level rise and what "Resilient Martin" is doing to mitigate those risks. | Not a member | Need representation from the Town in their stakeholder/steering committee group. | No one is currently serving | No |  | Does the Council wish to appoint a designated liaison and an alternate to assist "Resilient Martin" on their stakeholder / steering committee group? Contact Resilient Martin at (772) 288-5927 for meeting schedule. |  |

| | Organization | Town's status | Is the Town entitled to official representation on the organization's board? | If yes, who is currently serving? | Have any Town elected officials, not serving as an official representative, been involved with the organization? | If yes, who? | Comments | Action taken at January 13, 2025 Regular Town Council Meeting |
|---|---|---|---|---|---|---|---|---|
| 14 | **Jensen Beach Chamber of Commerce (JBCC) -** Chambers of Commerce main activities are, among others, safeguarding business interests and sharing business experiences and business interests, contact with governments, civil society, local media and the press and organzing trade shows and events. | Paying Member ($250) | No | NA | Yes | Mayor and Council Members routinely attend events. | It is assumed the Town Council members and Mayor will continue to participate in various Chamber events at their own initiative. | Participate at the discretion of Mayor and Town Council |
| 15 | **Invitations to official events, ribbon cuttings, State of the County Speech, etc.** | NA | NA | NA | NA | NA | Attendance at these types of events has been at the discretion of individual Council Members and the Mayor. Unless otherwise directed, staff will continue the role of informing everyone of events as they become known and assisting with reservations, RSVP's, etc. | Participation at the discretion of Mayor and Town Council |

Item#6

# Memorandum

TO: **TOWN COUNCIL AND MAYOR**

FROM: **HOLLY VATH, FINANCIAL CONSULTANT**

SUBJECT: **QUARTERLY FINANCIAL REPORT**

DATE: **DECEMBER 1, 2024**

Attached are the unaudited financial report for the 2024 fiscal year.

**Revenue**

The total budgeted revenue was $212,838, the Town received $244,209 which is $31,371 more than budgeted. The positive variance is generated from gas tax revenue and interest income. Additional gas tax funding will become restricted net assets, an additional $44,469 will be added to the Gas tax reserve. Gas tax funding must be utilized for transportation expenses such as street lighting and road maintenance. The 2024 budget anticipated utilization of $116,267 of reserves, the actual general fund reserve utilization was $105,577. The 2025 budget has seen an increase in state shared revenue. With the approval of an additional ½ cent sales tax by Martin County voters, the Town will see some additional revenue later in 2025 and for the next ten years.

**Expenditures**

The total budgeted expenditures were $329,105, the Town expended $305,316. General government expenses were below budget by $19,642 while Public Safety, which is mainly Building and Code compliance activity, was under budget by $2,533.

9:13 AM

11/21/24

Accrual Basis

# Town of Ocean Breeze General Fund
## Profit & Loss Budget vs. Actual
### October 2023 through September 2024

| | Oct '23 - Sep 24 | Budget | $ Over Budget |
|---|---|---|---|
| Ordinary Income/Expense | | | |
| Income | | | |
| 6001 · Taxes from other Governments | | | |
| 312300 · State Fuel Tax | 4,451.18 | 19,000.00 | -14,548.82 |
| 312410 · Local Option Gas Tax | 25,703.57 | 0.00 | 25,703.57 |
| 312420 · New Local Option Gas Tax | 18,700.38 | 0.00 | 18,700.38 |
| 314200 · Local Communications Svc Tax | 5,576.12 | 3,800.00 | 1,776.12 |
| 335120 · State Revenue Sharing | 18,382.44 | 23,000.00 | -4,617.56 |
| 335140 · Mobile Home Tags | 3,139.40 | 2,900.00 | 239.40 |
| 335150 · Alcoholic Beverage Licenses | 2,691.92 | 2,000.00 | 691.92 |
| 335180 · 1/2 Cent Sales Tax | 58,191.19 | 61,000.00 | -2,808.81 |
| Total 6001 · Taxes from other Governments | 136,836.20 | 111,700.00 | 25,136.20 |
| 6002 · Licenses & Permits | | | |
| 322000 · Building Permits | 17,934.87 | 20,000.00 | -2,065.13 |
| 338200 · Occupational Licenses | 569.54 | 400.00 | 169.54 |
| Total 6002 · Licenses & Permits | 18,504.41 | 20,400.00 | -1,895.59 |
| 6003 · Other Fees for Services | | | |
| 322001 · Fire Inspections | 0.00 | 500.00 | -500.00 |
| 322004 · Charges for Services | 174.00 | 0.00 | 174.00 |
| Total 6003 · Other Fees for Services | 174.00 | 500.00 | -326.00 |
| 6004 · Investment & Other Earnings | | | |
| 361000 · Interest Income | 24,276.83 | 16,000.00 | 8,276.83 |
| Total 6004 · Investment & Other Earnings | 24,276.83 | 16,000.00 | 8,276.83 |
| 6005 · Ad Valorem Revenue | | | |
| 312100 · Ad Valorem | 64,417.91 | 63,938.00 | 479.91 |
| Total 6005 · Ad Valorem Revenue | 64,417.91 | 63,938.00 | 479.91 |
| 6007 · Miscellaneous Income | | | |
| 369000 · Misc Inc - MCSB Admin Fee, Etc. | 0.00 | 300.00 | -300.00 |
| Total 6007 · Miscellaneous Income | 0.00 | 300.00 | -300.00 |
| Total Income | 244,209.35 | 212,838.00 | 31,371.35 |

# Town of Ocean Breeze General Fund
## Profit & Loss Budget vs. Actual
### October 2023 through September 2024

| | Oct '23 - Sep 24 | Budget | $ Over Budget |
|---|---|---|---|
| Expense | | | |
| 6101 · General Government | | | |
| 513150 · Gross Payroll | 48,042.00 | 55,600.00 | -7,558.00 |
| 513155 · PTO Accrual | 970.99 | 0.00 | 970.99 |
| 513297 · Grant Management Consultant | 0.00 | 0.00 | 0.00 |
| 513301 · Management Consultant | 23,656.00 | 28,000.00 | -4,344.00 |
| 513302 · Rent | 14,464.04 | 14,175.00 | 289.04 |
| 513304 · Communications / Website | 10,613.57 | 16,155.00 | -5,541.43 |
| 513305 · Engineering | 6,337.50 | 5,000.00 | 1,337.50 |
| 513306 · Accountant | 3,390.00 | 8,000.00 | -4,610.00 |
| 513308 · Insurance W/C | 1,429.00 | 5,000.00 | -3,571.00 |
| 513309 · Insurance Package | 25,042.00 | 24,300.00 | 742.00 |
| 513311 · Public Advertising Notices | 1,950.15 | 4,000.00 | -2,049.85 |
| 513312 · Office Equipment & Supplies | 12,604.97 | 10,230.00 | 2,374.97 |
| 513313 · Postage | 595.92 | 800.00 | -204.08 |
| 513314 · Petty Cash | 0.00 | 0.00 | 0.00 |
| 513315 · Audit | 16,250.00 | 16,500.00 | -250.00 |
| 513316 · Utilities | 599.85 | 720.00 | -120.15 |
| 513317 · Dues | 1,477.00 | 1,525.00 | -48.00 |
| 513318 · Mileage Reimb. - Clerks | 44.22 | 700.00 | -655.78 |
| 513319 · Conferences & Travel - Council | 6,194.84 | 6,800.00 | -605.16 |
| 513320 · Bank Fees | 0.00 | | |
| 513321 · Election Expenses | 653.90 | 1,000.00 | -346.10 |
| 513322 · Safety Deposit Box | 0.00 | 0.00 | 0.00 |
| 513324 · Special Project-Digitizing | 0.00 | 0.00 | 0.00 |
| 513325 · Meeting Security | 0.00 | 0.00 | 0.00 |
| 513326 · Special Projects | 13,345.61 | 5,000.00 | 8,345.61 |
| 513820 · Contributions | 300.00 | 1,000.00 | -700.00 |
| 514100 · Legal Counsel | 16,406.50 | 17,000.00 | -593.50 |
| 514200 · Computer Services | 5,919.99 | 6,900.00 | -980.01 |
| 531110 · Payroll Taxes - Fica | 2,978.64 | 4,200.00 | -1,221.36 |
| 531111 · Payroll Taxes - Medicare | 696.61 | 1,000.00 | -303.39 |
| 531112 · Benefits | 0.00 | 0.00 | 0.00 |
| Total 6101 · General Government | 213,963.30 | 233,605.00 | -19,641.70 |
| 6102 · Public Safety | | | |
| 524200 · Building Official Services | 20,512.50 | 27,000.00 | -6,487.50 |
| 524210 · Building Code Compliance Ser | 18,517.50 | 13,000.00 | 5,517.50 |
| 524220 · Code Compliance Legal | 23,840.00 | 24,000.00 | -160.00 |
| 524300 · Fire Safety Inspector | 0.00 | 500.00 | -500.00 |
| 524310 · Permit Processing Services | 24,097.50 | 25,000.00 | -902.50 |
| Total 6102 · Public Safety | 86,967.50 | 89,500.00 | -2,532.50 |

# Town of Ocean Breeze General Fund
## Profit & Loss Budget vs. Actual
### October 2023 through September 2024

| | Oct '23 - Sep 24 | Budget | $ Over Budget |
|---|---|---|---|
| 6104 · Transportation | | | |
| 541300 · Road and Street Maintenance | 2,965.00 | 3,500.00 | -535.00 |
| 541301 · Street Lights | 1,420.65 | 2,500.00 | -1,079.35 |
| 541400 · Sheriff Road Patrol | 0.00 | 0.00 | 0.00 |
| Total 6104 · Transportation | 4,385.65 | 6,000.00 | -1,614.35 |
| Total Expense | 305,316.45 | 329,105.00 | -23,788.55 |
| Net Ordinary Income | -61,107.10 | -116,267.00 | 55,159.90 |
| Other Income/Expense | | | |
| Other Expense | | | |
| 80000 · Ask My Accountant | 0.00 | | |
| Total Other Expense | 0.00 | | |
| Net Other Income | 0.00 | 0.00 | 0.00 |
| **Net Income** | **-61,107.10** | **-116,267.00** | **55,159.90** |

Item #7

# MEMORANDUM

TO: MAYOR OSTRAND AND MEMBERS OF THE TOWN COUNCIL

FROM: KIM STANTON, TOWN CLERK

SUBJECT: ADOPTION OF SAFEGUARDS AGAINST CYBERSECURITY THREATS

DATE: December 9, 2024

The State of Florida has directed local governments to adopt safeguards to guard against cybersecurity threats. The attached Resolution and its exhibits have been prepared in consultation with the state agency (Florida Digital Service) as well as our IT consultant, G Whiz Technologies, Inc. Staff has sought to propose regulations that are consistent with the Town's limited scope of exposure to cyber threats but also recognizes necessary steps for physical improvements.

Staff expects that over the remainder of this budget year, the first three of the six steps tasks identified within the resolution will be undertaken. We will attempt to absorb these costs within the existing budget and if unable to do so, a budget amendment will be sought in the coming months.

Staff recommends approval of Resolution No. 355-2024.

## Resolution No. 355-2024

**A RESOLUTION OF THE TOWN COUNCIL OF THE TOWN OF OCEAN BREEZE, FLORIDA, TO ADOPT STANDARDS TO SAFEGUARD AGAINST CYBERSECURITY THREATS; ADOPTING THE NIST CYBERSECURITY FRAMEWORK 2.0, PROMULGATED BY THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY; PROVIDING FOR CONFLICTS, SEVERABILITY, AND AN EFFECTIVE DATE.**

**Whereas,** Section 282.3185 (4) Florida Statutes provides that each local government shall adopt cybersecurity standards that safeguard its data, information technology, and information technology resources to ensure availability, confidentiality, and integrity; and

**Whereas,** Section 282.3185 (4) Florida Statute provides that each municipality with a population of less than 25,000 must adopt the cybersecurity standards required by this subsection by January 1, 2025; and

**Whereas,** the Town of Ocean Breeze must notify the Florida Digital Service of its compliance with this subsection as soon as possible; and

**Whereas,** the Town Council finds that the NIST Cybersecurity Framework 2.0 promulgated the National Institute of Standards and Technology provides standards that are consistent with generally accepted best practices for cybersecurity.

**NOW, THEREFORE, BE IT RESOLVED BY THE TOWN COUNCIL OF THE TOWN OF OCEAN BREEZE, FLORIDA, AS FOLLOWS:**

**Section I.** The foregoing findings are incorporated herein by reference and made a part hereof.

**Section II.** The standards which are set forth in the NIST Cybersecurity Framework 2.0, summarized by Exhibit A attached, and may be amended from time to time, which is promulgated by the National Institute of Standards and Technology, are hereby adopted by the Town to establish a framework for cybersecurity for the Town.

**Section III.** The Town shall establish cybersecurity policies and procedures intended to address the six functions outlined in the NIST Cyber Security Framework 2.0:

a) *Govern – establishing and monitoring cybersecurity risk management strategy, expectations, and policy.*

b) *Identify – determining the current cybersecurity risk to the town.*

c) *Protect – using safeguards, to prevent or reduce cybersecurity risk*.

d) *Detect – providing outcomes that help find and analyze possible cybersecurity attacks and compromises.*

e) *Respond – defining what actions to take when a cybersecurity incident is detected.*

f) *Recover – restoring assets and operations that were impacted by a cybersecurity incident.*

**Section IV.** Upon the Town's complying with the requirements set forth in Section 282.3185 (4) Florida Statutes, the Town Clerk shall notify the Florida Digital Service as soon as possible.

**Section V.** If any section or portion of a section of this Resolution proves to be invalid, unlawful, or unconstitutional, it shall not be held to invalidate or impair the validity, force, or effect of any other section or part of this Resolution.

**Section VI.** This Resolution shall be effective immediately upon its adoption.

**APPROVED AND ADOPTED** this 9TH day of December, 2024.

| | YES | NO | ABSENT |
|---|---|---|---|
| GEORGE CIASCHI, COUNCIL MEMBER | | | |
| KEVIN DOCHERTY, COUNCIL MEMBER | | | |
| JANET GALANTE, COUNCIL MEMBER | | | |
| MICHAEL HELLER, COUNCIL MEMBER | | | |
| SANDY KELLEY, COUNCIL MEMBER | | | |
| MATTHEW SQUIRES, COUNCIL MEMBER | | | |

**PASSED AND RESOLVED** by a ______vote of the Town Council of the Town of Ocean Breeze, Florida on this 9th day of December, 2024.

______________________________
**President:**

______________________________
**KAREN M. OSTRAND**
Mayor

**ATTEST:**

______________________________
**KIM STANTON**
Town Clerk

**APPROVED AS TO FORM AND LEGALITY:**

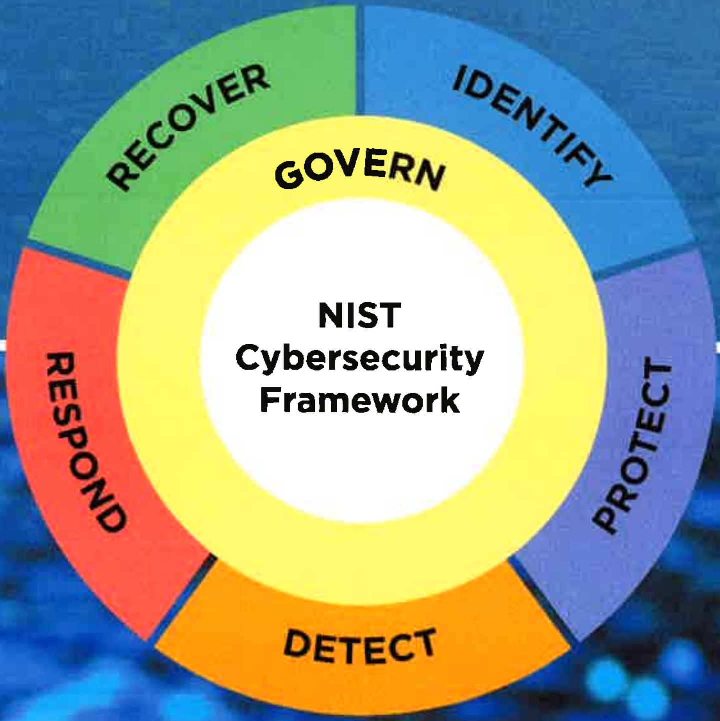
______________________________
**GEMMA TORCIVIA**
Town Attorney

Check for updates

NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Exhibit A

# NIST Cybersecurity Framework 2.0: RESOURCE & OVERVIEW GUIDE



NIST Special Publication
NIST SP 1299

https://doi.org/10.6028/NIST.SP.1299
February 2024

# NIST CSF 2.0:
# RESOURCE & OVERVIEW GUIDE

## WHAT IS THE CSF 2.0...AND POPULAR WAYS TO USE IT?

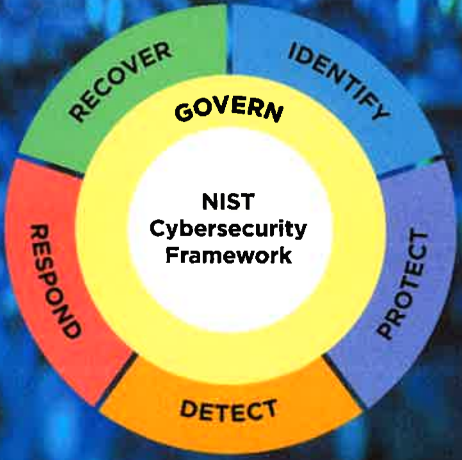
The NIST Cybersecurity Framework (CSF) 2.0 can help organizations manage and reduce their cybersecurity risks as they start or improve their cybersecurity program. The CSF outlines specific outcomes that organizations can achieve to address risk. Other NIST resources help explain specific actions that can be taken to achieve each outcome. *This guide is a supplement to the NIST CSF and is not intended to replace it.*

The CSF 2.0, along with NIST's supplementary resources, can be used by organizations to understand, assess, prioritize, and communicate cybersecurity risks; it is particularly useful for fostering internal and external communication across teams — as well as integrating with broader risk management strategies.

The CSF 2.0 is organized by six Functions — **Govern, Identify, Protect, Detect, Respond,** and **Recover.** Together, these Functions provide a comprehensive view for managing cybersecurity risk. This *Resource & Overview Guide* offers details about each Function to serve as potential starting points.

The CSF 2.0 is comprised of:

- **CSF Core** - A taxonomy of high-level cybersecurity outcomes that can help any organization manage its cybersecurity risks.
- **CSF Organizational Profiles** - A mechanism for describing an organization's current and/or target cybersecurity posture in terms of the CSF Core's outcomes.
- **CSF Tiers** - Can be applied to CSF Organizational Profiles to characterize the rigor of an organization's cybersecurity risk governance and management practices.



# NIST CSF 2.0:
# RESOURCE & OVERVIEW GUIDE

## EXPLORE MORE CSF 2.0 RESOURCES

| | |
|---|---|
| Informative References | **View and create mappings between CSF 2.0 and other documents.** Do you want to submit your mappings to NIST documents and have them displayed on our site? Please follow the link to the left or email olir@nist.gov if you have any questions. |
| Cybersecurity & Privacy Reference Tool (CPRT) | **Browse and download the CSF 2.0 Core & mapped content**. CPRT provides a centralized, standardized, and modernized mechanism for managing reference datasets (and offers a consistent format for accessing reference data from various NIST cybersecurity and privacy standards, guidelines, and frameworks). |
| Implementation Examples | View and download notional examples of concise, action-oriented steps to help achieve the outcomes of the CSF 2.0 Subcategories in addition to the guidance provided in the Informative References. |
| CSF 2.0 Reference Tool | Access human and machine-readable versions of the Core (in JSON and Excel). You can also view and export portions of the Core using key search terms. |

**Additional Resources Include:**

Community Profiles and Profile templates (help organizations put the CSF into practice)

**Search tools** (simplify and streamline as you look for specific information)

**Concept papers** (learn more about various CSF topics)

**FAQs** (see what others are asking and get answers to top questions)

Explore the suite of NIST's CSF 2.0 Resource Repository

# NIST CSF 2.0:
# RESOURCE & OVERVIEW GUIDE

## NAVIGATING NIST's CSF 2.0 QUICK START GUIDES (QSG)

| QSG Type | Description | Explore |
|---|---|---|
| Small Business (SMB) | Provides SMBs, specifically those who have modest or no cybersecurity plans in place, with considerations to kick-start their cybersecurity risk management strategy. | See the QSG |
| Creating and Using Organizational Profiles | Provides all organizations with considerations for creating and using Current and/or Target Profiles to implement the CSF 2.0. | See the QSG |
| Using the CSF Tiers | Explains how any organization can apply the CSF Tiers to Organizational Profiles to characterize the rigor of its cybersecurity risk governance and management practices. | See the QSG |
| Draft Cybersecurity Supply Chain Risk Management (C-SCRM) | Helps all organizations to become smart acquirers and suppliers of technology products and services by improving their C-SCRM processes. | See the QSG |
| Draft Enterprise Risk Management (ERM) Practitioners | Details how Enterprise Risk Management practitioners can utilize the outcomes provided in CSF 2.0 to improve organizational cybersecurity risk management. | See the QSG |

**...and more to follow in the future.**

See the current online QSG repository

# NIST CSF 2.0: RESOURCE & OVERVIEW GUIDE

## GOVERN

The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.

**Understand and assess specific cybersecurity needs.** Determine your organization's unique risks and needs. Discuss the current and predicted risk environment and the amount of risk your organization is willing to accept. Seek input and ideas from across the organization. Understand what has worked or not worked well in the past and discuss it openly.

**Develop a tailored cybersecurity risk strategy.** This should be based on your organization's specific cybersecurity objectives, the risk environment, and lessons learned from the past — and from others. Manage, update, and discuss the strategy at regular intervals. Roles and responsibilities should be clear.

**Establish defined risk management policies.** Policies should be approved by management and should be organization-wide, repeatable, and recurring, and should align with the current cybersecurity threat environment, risks (which will change over time), and mission objectives. Embed policies in company culture to help drive and inspire the ability to make informed decisions. Account for legal, regulatory, and contractual obligations.

**Develop and communicate organizational cybersecurity practices.** These must be straightforward and communicated regularly. They should reflect the application of risk management to changes in mission or business requirements, threats, and overall technical landscape. Document practices and share them with room for feedback and the agility to change course.

**Establish and monitor cybersecurity supply chain risk management.** Establish strategy, policy, and roles and responsibilities — including for overseeing suppliers, customers, and partners. Incorporate requirements into contracts. Involve partners and suppliers in planning, response, and recovery.

**Implement continuous oversight and checkpoints.** Analyze risks at regular intervals and monitor them continuously (just as you would with financial risks).

## IDENTIFY

The organization's current cybersecurity risks are understood.

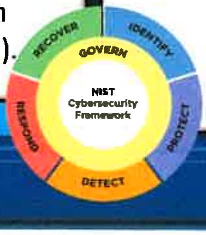
**Identify critical business processes and assets.** Consider which of your organization's activities absolutely must continue to be viable. For example, this could be maintaining a website to retrieve payments, securely protecting customer/patient information, or ensuring that the information critical to your organization remains accessible and accurate.

**Maintain inventories of hardware, software, services, and systems.** Know what computers and software your organization uses — including services provided by suppliers — because these are frequently the entry points of malicious actors. This inventory could be as simple as a spreadsheet. Consider including owned, leased, and employees' personal devices and apps.

**Document information flows.** Consider what type of information your organization collects and uses (and where the data are located and how they are used), especially when contracts and external partners are involved.

**Identify threats, vulnerabilities, and risk to assets.** Informed by knowledge of internal and external threats, risks should be identified, assessed, and documented. Examples of ways to document them include risk registers – repositories of risk information, including data about risks over time. Ensure risk responses are identified, prioritized, and executed, and that results are monitored.

**Lessons learned are used to identify improvements.** When conducting day-to-day business operations, it is important to identify ways to further refine or enhance performance, including opportunities to better manage and reduce cybersecurity risks. This requires purposeful effort by your organization at all levels. If there is an incident, assess what happened. Prepare an after-action report that documents the incident, the response, recovery actions taken, and lessons learned.



# NIST CSF 2.0: RESOURCE & OVERVIEW GUIDE

## PROTECT

Safeguards to manage the organization's cybersecurity risks are used.

**Manage access.** Create unique accounts for employees and ensure users only have access to necessary resources. Authenticate users before they are granted access to information, computers, and applications. Manage and track physical access to facilities/devices.

**Train users.** Regularly train employees to ensure they are aware of cybersecurity policies and procedures and that they have the knowledge and skills to perform general and specific tasks; explain how to recognize common attacks and report suspicious activity. Certain roles may require extra training.

**Protect and monitor your devices.** Consider using endpoint security products. Apply uniform configurations to devices and control changes to device configurations. Disable services or features that don't support mission functions. Configure systems and services to generate log records. Ensure devices are disposed of securely.

**Protect sensitive data.** Ensure sensitive stored or transmitted data are protected by encryption. Consider utilizing integrity checking so only approved changes are made to data. Securely delete and/or destroy data when no longer needed or required.

**Manage and maintain software.** Regularly update operating systems and applications; enable automatic updates. Replace end-of-life software with supported versions. Consider using software tools to scan devices for additional vulnerabilities and remediate them.

**Conduct regular backups.** Back up data at agreed-upon schedules or use built-in backup capabilities; software and cloud solutions can automate this process. Keep at least one frequently backed-up set of data offline to protect it against ransomware. Test to ensure that backed-up data can be successfully restored to systems.

## DETECT

Possible cybersecurity attacks and compromises are found and analyzed.

**Monitor networks, systems, and facilities continuously to find potentially adverse events.** Develop and test processes and procedures for detecting indicators of a cybersecurity incident on the network and in the physical environment. Collect log information from multiple organizational sources to assist in detecting unauthorized activity.

**Determine and analyze the estimated impact and scope of adverse events.** If a cybersecurity event is detected, your organization should work quickly and thoroughly to understand the impact of the incident. Understanding details regarding any cybersecurity incidents will help inform the response.

**Provide information on adverse events to authorized staff and tools.** When adverse events are detected, provide information about the event internally to authorized personnel to ensure appropriate incident response actions are taken.

# NIST CSF 2.0: RESOURCE & OVERVIEW GUIDE

## RESPOND

Actions regarding a detected cybersecurity incident are taken.

**Execute an incident response plan once an incident is declared, in coordination with relevant third parties.** To properly execute an incident response plan, ensure everyone knows their responsibilities; this includes understanding any requirements (e.g., regulatory, legal reporting, and information sharing).

**Categorize and prioritize incidents and escalate or elevate as needed.** Analyze what has been taking place, determine the root cause of the incident, and prioritize which incidents require attention first from your organization. Communicate this prioritization to your team and ensure everyone understands who information should be communicated to regarding a prioritized incident when it occurs.

**Collect incident data and preserve its integrity and provenance.** Collecting information in a safe manner will help in your organization's response to an incident. Ensure that data are still secure after the incident to maintain your organization's reputation and trust from stakeholders. Storing this information in a safe manner can also help inform updated and future response plans to be even more effective.

**Notify internal and external stakeholders of any incidents and share incident information with them — following policies set by your organization.** Securely share information consistent with response plans and information-sharing agreements. Notify business partners and customers of incidents in accordance with contractual requirements.

**Contain and eradicate incidents.** Executing a developed and tested response plan will help your organization contain the effects of an incident and eradicate it. Meaningful coordination and communication with stakeholders can result in a more effective response and mitigation of the incident.

## RECOVER

Assets and operations affected by a cybersecurity incident are restored.

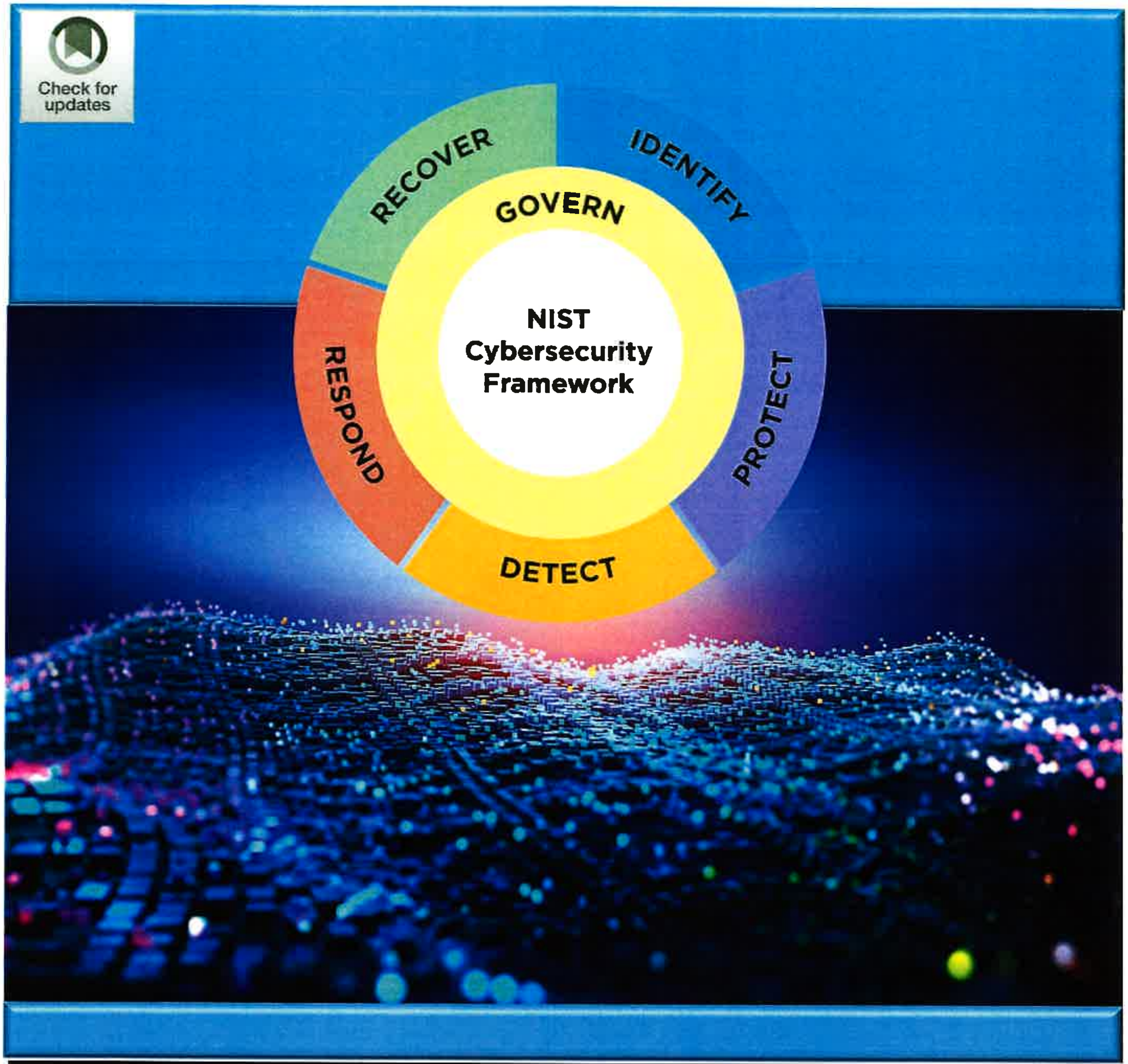
**Understand roles and responsibilities.** Understand who, within and outside your business, has recovery responsibilities. Know who has access and authority to make decisions to carry out your response efforts on behalf of the business.

**Execute your recovery plan.** Ensure operational availability of affected systems and services; and prioritize and perform recovery tasks.

**Double-check your work.** It is important to ensure the integrity of backups and other recovery assets before using them to resume regular business operations.

**Communicate with internal and external stakeholders.** Carefully account for what, how, and when information will be shared with various stakeholders so that all interested parties receive the information they need, but no inappropriate information is shared. Communicate to your staff any lessons learned and revisions to processes, procedures, and technologies (following policies already set by the organization). This is a good time to train, or retrain, staff on cybersecurity best practices.

Check for updates



# The NIST Cybersecurity Framework (CSF) 2.0

National Institute of Standards and Technology
This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.29

February 26, 2024

NIST
NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

## Abstract

The NIST Cybersecurity Framework (CSF) 2.0 provides guidance to industry, government agencies, and other organizations to manage cybersecurity risks. It offers a taxonomy of high-level cybersecurity outcomes that can be used by any organization — regardless of its size, sector, or maturity — to better understand, assess, prioritize, and communicate its cybersecurity efforts. The CSF does not prescribe how outcomes should be achieved. Rather, it links to online resources that provide additional guidance on practices and controls that could be used to achieve those outcomes. This document describes CSF 2.0, its components, and some of the many ways that it can be used.

## Keywords

cybersecurity; Cybersecurity Framework (CSF); cybersecurity risk governance; cybersecurity risk management; enterprise risk management; Profiles; Tiers.

## Audience

Individuals responsible for developing and leading cybersecurity programs are the primary audience for the CSF. The CSF can also be used by others involved in managing risk — including executives, boards of directors, acquisition professionals, technology professionals, risk managers, lawyers, human resources specialists, and cybersecurity and risk management auditors — to guide their cybersecurity-related decisions. Additionally, the CSF can be useful to those making and influencing policy (e.g., associations, professional organizations, regulators) who set and communicate priorities for cybersecurity risk management.

## Supplemental Content

NIST will continue to build and host additional resources to help organizations implement the CSF, including Quick Start Guides and Community Profiles. All resources are made publicly available on the NIST CSF website. Suggestions for additional resources to reference on the NIST CSF website can always be shared with NIST at cyberframework@nist.gov.

## Note to Readers

Unless otherwise noted, documents cited, referenced, or excerpted in this publication are not wholly incorporated into this publication.

Before version 2.0, the Cybersecurity Framework was called the "Framework for Improving Critical Infrastructure Cybersecurity." This title is not used for CSF 2.0.

## Acknowledgments

The CSF is the result of a multi-year collaborative effort across industry, academia, and government in the United States and around the world. NIST acknowledges and thanks all of those who have contributed to this revised CSF. Information on the CSF development process can be found on the NIST CSF website. Lessons learned about the use of the CSF can always be shared with NIST at cyberframework@nist.gov.

## Table of Contents

## List of Figures

## Preface

The Cybersecurity Framework (CSF) 2.0 is designed to help organizations of all sizes and sectors — including industry, government, academia, and nonprofit — to manage and reduce their cybersecurity risks. It is useful regardless of the maturity level and technical sophistication of an organization's cybersecurity programs. Nevertheless, the CSF does not embrace a one-size-fits-all approach. Each organization has both common and unique risks, as well as varying risk appetites and tolerances, specific missions, and objectives to achieve those missions. By necessity, the way organizations implement the CSF will vary.

Ideally, the CSF will be used to address cybersecurity risks alongside other risks of the enterprise, including those that are financial, privacy, supply chain, reputational, technological, or physical in nature.

The CSF *describes* desired outcomes that are intended to be understood by a broad audience, including executives, managers, and practitioners, regardless of their cybersecurity expertise. Because these outcomes are sector-, country-, and technology-neutral, they provide an organization with the flexibility needed to address their unique risks, technologies, and mission considerations. Outcomes are mapped directly to a list of potential security controls for immediate consideration to mitigate cybersecurity risks.

Although not prescriptive, the CSF assists its users in learning about and selecting specific outcomes. Suggestions for how specific outcomes may be achieved are provided in an expanding suite of online resources that complement the CSF, including a series of Quick Start Guides (QSGs). Also, various tools offer downloadable formats to help organizations that choose to automate some of their processes. The QSGs suggest initial ways to use the CSF and invite the reader to explore the CSF and related resources in greater depth. Available through the NIST CSF website, the CSF and these supplementary resources from NIST and others should be viewed as a "CSF portfolio" to help manage and reduce risks. Regardless of how it is applied, the CSF prompts its users to consider their cybersecurity posture in context and then adapt the CSF to their specific needs.

Building on previous versions, CSF 2.0 contains new features that highlight the importance of *governance* and *supply chains*. Special attention is paid to the QSGs to ensure that the CSF is relevant and readily accessible by smaller organizations as well as their larger counterparts. NIST now provides *Implementation Examples* and *Informative References*, which are available online and updated regularly. Creating current and target state *Organizational Profiles* helps organizations to compare where they are versus where they want or need to be and allows them to implement and assess security controls more quickly.

Cybersecurity risks are expanding constantly, and managing those risks must be a continuous process. This is true regardless of whether an organization is just beginning to confront its cybersecurity challenges or whether it has been active for many years with a sophisticated, well-resourced cybersecurity team. The CSF is designed to be valuable for any type of organization and is expected to provide appropriate guidance over a long time.

## 1. Cybersecurity Framework (CSF) Overview

This document is version 2.0 of the NIST Cybersecurity Framework (*Framework* or *CSF*). It includes the following components:

- ***CSF Core***, the nucleus of the CSF, which is a taxonomy of high-level cybersecurity outcomes that can help any organization manage its cybersecurity risks. The CSF Core components are a hierarchy of Functions, Categories, and Subcategories that detail each outcome. These outcomes can be understood by a broad audience, including executives, managers, and practitioners, regardless of their cybersecurity expertise. Because the outcomes are sector-, country-, and technology-neutral, they provide an organization with the flexibility needed to address its unique risks, technologies, and mission considerations.
- ***CSF Organizational Profiles***, which are a mechanism for describing an organization's current and/or target cybersecurity posture in terms of the CSF Core's outcomes.
- ***CSF Tiers***, which can be applied to CSF Organizational Profiles to characterize the rigor of an organization's cybersecurity risk governance and management practices. Tiers can also provide context for how an organization views cybersecurity risks and the processes in place to manage those risks.

This document describes *what* desirable outcomes an organization can aspire to achieve. It does not *prescribe* outcomes nor *how* they may be achieved. Descriptions of *how* an organization can achieve those outcomes are provided in a suite of online resources that complement the CSF and are available through the NIST CSF website. These resources offer additional guidance on practices and controls that could be used to achieve outcomes and are intended to help an organization understand, adopt, and use the CSF. They include:

- *Informative References* that point to sources of guidance on each outcome from existing global standards, guidelines, frameworks, regulations, policies, etc.
- *Implementation Examples* that illustrate potential ways to achieve each outcome
- *Quick-Start Guides* that give actionable guidance on using the CSF and its online resources, including transitioning from previous CSF versions to version 2.0
- *Community Profiles* and *Organizational Profile Templates* that help an organization put the CSF into practice and set priorities for managing cybersecurity risks

An organization can use the CSF Core, Profiles, and Tiers with the supplementary resources to understand, assess, prioritize, and communicate cybersecurity risks.

- **Understand and Assess:** Describe the current or target cybersecurity posture of part or all of an organization, determine gaps, and assess progress toward addressing those gaps.

- **Prioritize:** Identify, organize, and prioritize actions for managing cybersecurity risks that align with the organization's mission, legal and regulatory requirements, and risk management and governance expectations.
- **Communicate:** Provide a common language for communicating inside and outside the organization about cybersecurity risks, capabilities, needs, and expectations.

The CSF is designed to be used by organizations of all sizes and sectors, including industry, government, academia, and nonprofit organizations, regardless of the maturity level of their cybersecurity programs. The CSF is a foundational resource that may be adopted voluntarily and through governmental policies and mandates. The CSF's taxonomy and referenced standards, guidelines, and practices are not country-specific, and previous versions of the CSF have been leveraged successfully by many governments and other organizations both inside and outside of the United States.

The CSF should be used in conjunction with other resources (e.g., frameworks, standards, guidelines, leading practices) to better manage cybersecurity risks and inform the overall management of information and communications technology (ICT) risks at an enterprise level. The CSF is a flexible framework that is intended to be tailored for use by all organizations regardless of size. Organizations will continue to have unique risks — including different threats and vulnerabilities — and risk tolerances, as well as unique mission objectives and requirements. Thus, organizations' approaches to managing risks and their implementations of the CSF will vary.

The remainder of this document is structured as follows:

- Section 2 explains the basics of the CSF Core: Functions, Categories, and Subcategories.
- Section 3 defines the concepts of CSF Profiles and Tiers.
- Section 4 provides an overview of selected components of the CSF's suite of online resources: Informative References, Implementation Examples, and Quick Start Guides.
- Section 5 discusses how an organization can integrate the CSF with other risk management programs.
- Appendix A is the CSF Core.
- Appendix B contains a notional illustration of the CSF Tiers.
- Appendix C is a glossary of CSF terminology.

## 2. Introduction to the CSF Core

Appendix A is the CSF Core — a set of cybersecurity outcomes arranged by Function, then Category, and finally Subcategory, as depicted in Fig. 1. These outcomes are not a checklist of actions to perform; specific actions taken to achieve an outcome will vary by organization and use case, as will the individual responsible for those actions. Additionally, the order and size of Functions, Categories, and Subcategories in the Core does not imply the sequence or importance of achieving them. The structure of the Core is intended to resonate most with those charged with operationalizing risk management within an organization.

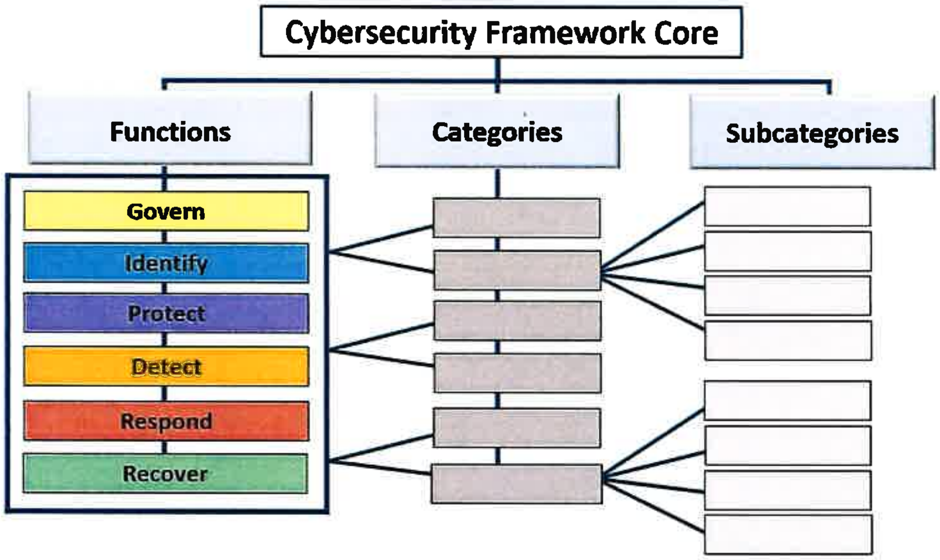


**Fig. 1. CSF Core structure**

The CSF Core Functions — Govern, Identify, Protect, Detect, Respond, and Recover — organize cybersecurity outcomes at their highest level.

- **Govern (GV)** — *The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.* The Govern Function provides outcomes to inform what an organization may do to achieve and prioritize the outcomes of the other five Functions in the context of its mission and stakeholder expectations. Governance activities are critical for incorporating cybersecurity into an organization's broader enterprise risk management (ERM) strategy. Govern addresses an understanding of organizational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policy; and the oversight of cybersecurity strategy.

- **Identify (ID)** — *The organization's current cybersecurity risks are understood.* Understanding the organization's assets (e.g., data, hardware, software, systems, facilities, services, people), suppliers, and related cybersecurity risks enables an organization to prioritize its efforts consistent with its risk management strategy and the mission needs identified under Govern. This Function also includes the identification of improvement opportunities for the organization's policies, plans, processes, procedures, and practices that support cybersecurity risk management to inform efforts under all six Functions.

- **PROTECT (PR)** — *Safeguards to manage the organization's cybersecurity risks are used.* Once assets and risks are identified and prioritized, PROTECT supports the ability to secure those assets to prevent or lower the likelihood and impact of adverse cybersecurity events, as well as to increase the likelihood and impact of taking advantage of opportunities. Outcomes covered by this Function include identity management, authentication, and access control; awareness and training; data security; platform security (i.e., securing the hardware, software, and services of physical and virtual platforms); and the resilience of technology infrastructure.
- **DETECT (DE)** — *Possible cybersecurity attacks and compromises are found and analyzed.* DETECT enables the timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse events that may indicate that cybersecurity attacks and incidents are occurring. This Function supports successful incident response and recovery activities.
- **RESPOND (RS)** — *Actions regarding a detected cybersecurity incident are taken.* RESPOND supports the ability to contain the effects of cybersecurity incidents. Outcomes within this Function cover incident management, analysis, mitigation, reporting, and communication.
- **RECOVER (RC)** — *Assets and operations affected by a cybersecurity incident are restored.* RECOVER supports the timely restoration of normal operations to reduce the effects of cybersecurity incidents and enable appropriate communication during recovery efforts.

> While many cybersecurity risk management activities focus on preventing negative events from occurring, they may also support taking advantage of positive opportunities. Actions to reduce cybersecurity risk might benefit an organization in other ways, like increasing revenue (e.g., first offering excess facility space to a commercial hosting provider for hosting their own and other organizations' data centers, then moving a major financial system from the organization's in-house data center to the hosting provider to reduce cybersecurity risks).

Figure 2 shows the CSF Functions as a wheel because all of the Functions relate to one another. For example, an organization will categorize assets under IDENTIFY and take steps to secure those assets under PROTECT. Investments in planning and testing in the GOVERN and IDENTIFY Functions will support timely detection of unexpected events in the DETECT Function, as well as enabling incident response and recovery actions for cybersecurity incidents in the RESPOND and RECOVER Functions. GOVERN is in the center of the wheel because it informs how an organization will implement the other five Functions.

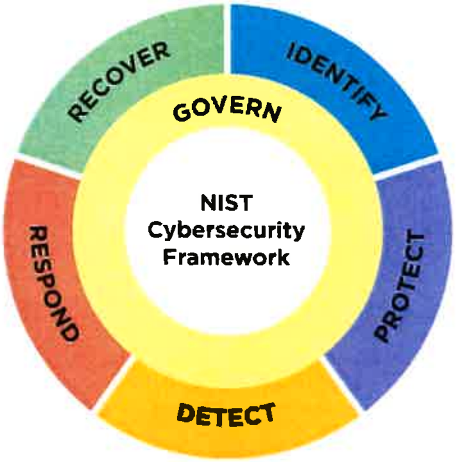


**Fig. 2. CSF Functions**

The Functions should be addressed concurrently. Actions that support Govern, Identify, Protect, and Detect should all happen continuously, and actions that support Respond and Recover should be ready at all times and happen when cybersecurity incidents occur. All Functions have vital roles related to cybersecurity incidents. Govern, Identify, and Protect outcomes help prevent and prepare for incidents, while Govern, Detect, Respond, and Recover outcomes help discover and manage incidents.

Each Function is named after a verb that summarizes its contents. Each Function is divided into *Categories*, which are related cybersecurity outcomes that collectively comprise the Function. *Subcategories* further divide each Category into more specific outcomes of technical and management activities. The Subcategories are not exhaustive, but they describe detailed outcomes that support each Category.

The Functions, Categories, and Subcategories apply to all ICT used by an organization, including information technology (IT), the Internet of Things (IoT), and operational technology (OT). They also apply to all types of technology environments, including cloud, mobile, and artificial intelligence systems. The CSF Core is forward-looking and intended to apply to future changes in technologies and environments.

## 3. Introduction to CSF Profiles and Tiers

This section defines the concepts of CSF Profiles and Tiers.

### 3.1. CSF Profiles

A *CSF Organizational Profile* describes an organization's current and/or target cybersecurity posture in terms of the Core's outcomes. Organizational Profiles are used to understand, tailor, assess, prioritize, and communicate the Core's outcomes by considering an organization's mission objectives, stakeholder expectations, threat landscape, and requirements. An organization can then prioritize its actions to achieve specific outcomes and communicate that information to stakeholders.

Every Organizational Profile includes one or both of the following:

1. A *Current Profile* specifies the Core outcomes that an organization is currently achieving (or attempting to achieve) and characterizes how or to what extent each outcome is being achieved.
2. A *Target Profile* specifies the desired outcomes that an organization has selected and prioritized for achieving its cybersecurity risk management objectives. A Target Profile considers anticipated changes to the organization's cybersecurity posture, such as new requirements, new technology adoption, and threat intelligence trends.

A *Community Profile* is a baseline of CSF outcomes that is created and published to address shared interests and goals among a number of organizations. A Community Profile is typically developed for a particular sector, subsector, technology, threat type, or other use case. An organization can use a Community Profile as the basis for its own Target Profile. Examples of Community Profiles can be found on the NIST CSF website.

The steps shown in Fig. 3 and summarized below illustrate one way that an organization could use an Organizational Profile to help inform continuous improvement of its cybersecurity.

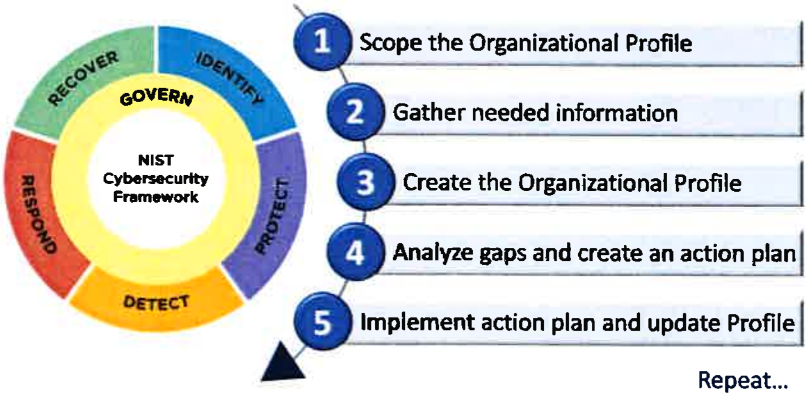

RECOVER
IDENTIFY
GOVERN
NIST Cybersecurity Framework
RESPOND
PROTECT
DETECT
1 Scope the Organizational Profile
2 Gather needed information
3 Create the Organizational Profile
4 Analyze gaps and create an action plan
5 Implement action plan and update Profile
Repeat...

**Fig. 3. Steps for creating and using a CSF Organizational Profile**

1. **Scope the Organizational Profile.** Document the high-level facts and assumptions on which the Profile will be based to define its scope. An organization can have as many Organizational Profiles as desired, each with a different scope. For example, a Profile could address an entire organization or be scoped to an organization's financial systems or to countering ransomware threats and handling ransomware incidents involving those financial systems.
2. **Gather the information needed to prepare the Organizational Profile.** Examples of information may include organizational policies, risk management priorities and resources, enterprise risk profiles, business impact analysis (BIA) registers, cybersecurity requirements and standards followed by the organization, practices and tools (e.g., procedures and safeguards), and work roles.
3. **Create the Organizational Profile.** Determine what types of information the Profile should include for the selected CSF outcomes, and document the needed information. Consider the risk implications of the Current Profile to inform Target Profile planning and prioritization. Also, consider using a Community Profile as the basis for the Target Profile.
4. **Analyze the gaps between the Current and Target Profiles, and create an action plan.** Conduct a gap analysis to identify and analyze the differences between the Current and Target Profiles, and develop a prioritized action plan (e.g., risk register, risk detail report, Plan of Action and Milestones [POA&M]) to address those gaps.
5. **Implement the action plan, and update the Organizational Profile.** Follow the action plan to address the gaps and move the organization toward the Target Profile. An action plan may have an overall deadline or be ongoing.

Given the importance of continual improvement, an organization can repeat these steps as often as needed.

There are additional uses for Organizational Profiles. For example, a Current Profile can be used to document and communicate the organization's cybersecurity capabilities and known opportunities for improvement with external stakeholders, such as business partners or prospective customers. Also, a Target Profile can help express the organization's cybersecurity risk management requirements and expectations to suppliers, partners, and other third parties as a target for those parties to achieve.

### 3.2. CSF Tiers

An organization can choose to use the Tiers to inform its Current and Target Profiles. *Tiers* characterize the rigor of an organization's cybersecurity risk governance and management practices, and they provide context for how an organization views cybersecurity risks and the processes in place to manage those risks. The Tiers, as shown in Fig. 4 and notionally illustrated in Appendix B, reflect an organization's practices for managing cybersecurity risk as Partial (Tier 1), Risk Informed (Tier 2), Repeatable (Tier 3), and Adaptive (Tier 4). The Tiers describe a progression from informal, ad hoc responses to approaches that are agile, risk-informed, and continuously improving. Selecting Tiers helps set the overall tone for how an organization will manage its cybersecurity risks.

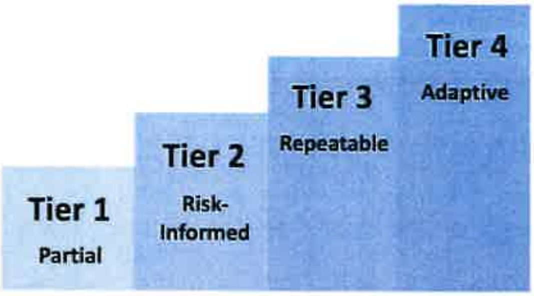


**Fig. 4. CSF Tiers for cybersecurity risk governance and management**

Tiers should complement an organization's cybersecurity risk management methodology rather than replace it. For example, an organization can use the Tiers to communicate internally as a benchmark for an organization-wide[1] approach to managing cybersecurity risks. Progression to higher Tiers is encouraged when risks or mandates are greater or when a cost-benefit analysis indicates a feasible and cost-effective reduction of negative cybersecurity risks.

The NIST CSF website provides additional information on using Profiles and Tiers. It includes pointers to NIST-hosted Organizational Profile templates and a repository of Community Profiles in a variety of machine-readable and human-usable formats.

[1] For the purposes of this document, the terms "organization-wide" and "enterprise" have the same meaning.

## 4. Introduction to Online Resources That Supplement the CSF

NIST and other organizations have produced a suite of online resources that help organizations understand, adopt, and use the CSF. Since they are hosted online, these additional resources can be updated more frequently than this document, which is updated infrequently to provide stability to its users, and be available in machine-readable formats. This section provides an overview of three types of online resources: Informative References, Implementation Examples, and Quick Start Guides.

*Informative References* are mappings that indicate relationships between the Core and various standards, guidelines, regulations, and other content. Informative References help inform how an organization may achieve the Core's outcomes. Informative References can be sector- or technology-specific. They may be produced by NIST or another organization. Some Informative References are narrower in scope than a Subcategory. For example, a particular control from SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, may be one of many references needed to achieve the outcome described in one Subcategory. Other Informative References may be higher-level, such as a requirement from a policy that partially addresses numerous Subcategories. When using the CSF, an organization can identify the most relevant Informative References.

*Implementation Examples* provide notional examples of concise, action-oriented steps to help achieve the outcomes of the Subcategories. Verbs used to express Examples include share, document, develop, perform, monitor, analyze, assess, and exercise. The Examples are not a comprehensive list of all actions that could be taken by an organization to achieve an outcome, nor do they represent a baseline of required actions to address cybersecurity risks.

*Quick-Start Guides (QSGs)* are brief documents on specific CSF-related topics and are often tailored to specific audiences. QSGs can help an organization implement the CSF because they distill specific portions of the CSF into actionable "first steps" that an organization can consider on the path to improving their cybersecurity posture and management of associated risks. The guides are revised in their own time frames, and new guides are added as needed.

Suggestions for new Informative References for CSF 2.0 can always be shared with NIST at olir@nist.gov. Suggestions for other resources to reference on the NIST CSF website, including additional QSG topics, should be directed to cyberframework@nist.gov.

## 5. Improving Cybersecurity Risk Communication and Integration

The CSF's use will vary based on an organization's unique mission and risks. With an understanding of stakeholder expectations and risk appetite and tolerance (as outlined in GOVERN), an organization can prioritize cybersecurity activities to make informed decisions about cybersecurity expenditures and actions. An organization may choose to handle risk in one or more ways — including mitigating, transferring, avoiding, or accepting negative risks and realizing, sharing, enhancing, or accepting positive risks — depending on the potential impacts and likelihoods. Importantly, an organization can use the CSF both internally to manage its cybersecurity capabilities and externally to oversee or communicate with third parties.

Regardless of the CSF's utilization, an organization may benefit from using the CSF as guidance to help it understand, assess, prioritize, and communicate cybersecurity risks and the actions that will manage those risks. The selected outcomes can be used to focus on and implement strategic decisions to improve cybersecurity postures and maintain continuity of mission-essential functions while taking priorities and available resources into account.

### 5.1. Improving Risk Management Communication

The CSF provides a basis for improved communication regarding cybersecurity expectations, planning, and resources. The CSF fosters bidirectional information flow (as shown in the top half of Fig. 5) between executives who focus on the organization's priorities and strategic direction and managers who manage specific cybersecurity risks that could affect the achievement of those priorities. The CSF also supports a similar flow (as shown in the bottom half of Fig. 5) between managers and the practitioners who implement and operate the technologies. The left side of the figure indicates the importance of practitioners sharing their updates, insights, and concerns with managers and executives.

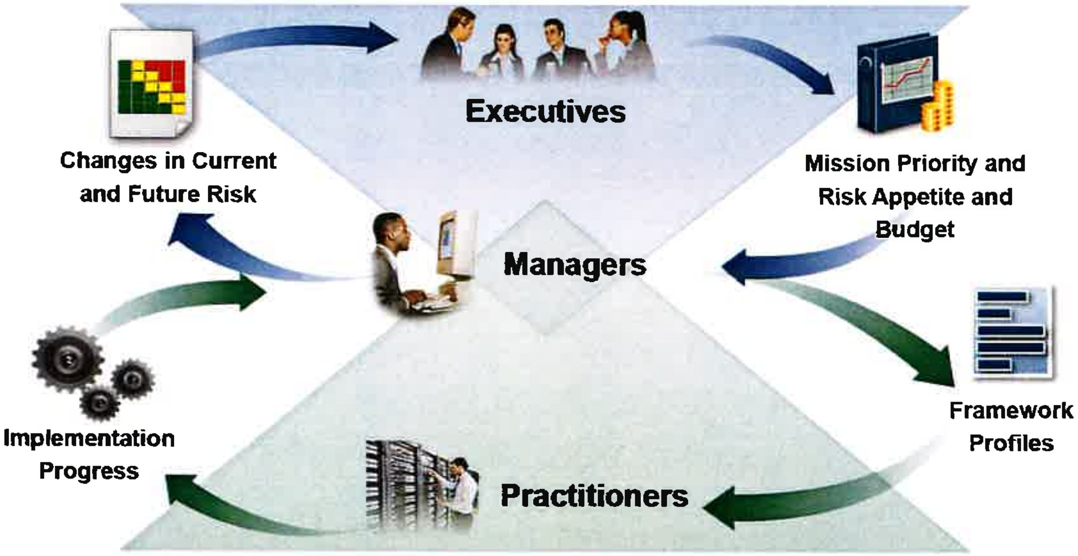

Executives
Changes in Current and Future Risk
Mission Priority and Risk Appetite and Budget
Managers
Framework Profiles
Implementation Progress
Practitioners

Fig. 5. Using the CSF to improve risk management communication

Preparing to create and use Organizational Profiles involves gathering information about organizational priorities, resources, and risk direction from executives. Managers then collaborate with practitioners to communicate business needs and create risk-informed Organizational Profiles. Actions to close any gaps identified between the Current and Target Profiles will be implemented by managers and practitioners and will provide key inputs into system-level plans. As the target state is achieved throughout the organization — including through controls and monitoring applied at the system level — the updated results can be shared through risk registers and progress reports. As part of ongoing assessment, managers gain insights to make adjustments that further reduce potential harms and increase potential benefits.

The GOVERN Function supports organizational risk communication with **executives**. Executives' discussions involve strategy, particularly how cybersecurity-related uncertainties might affect the achievement of organizational objectives. These governance discussions support dialogue and agreement about risk management strategies (including cybersecurity supply chain risk); roles, responsibilities, and authorities; policies; and oversight. As executives establish cybersecurity priorities and objectives based on those needs, they communicate expectations about risk appetite, accountability, and resources. Executives are also responsible for integrating cybersecurity risk management with ERM programs and lower-level risk management programs (see Sec. 5.2). The communications reflected in the top half of Fig. 5 can include considerations for ERM and the lower-level programs and, thus, inform managers and practitioners.

The overall cybersecurity objectives set by executives are informed by and cascade to **managers**. In a commercial entity, these may apply to a line-of-business or operating division. For government entities, these may be division- or branch-level considerations. When implementing the CSF, managers will focus on how to achieve risk targets through common services, controls, and collaboration, as expressed in the Target Profile and improved through the actions being tracked in the action plan (e.g., risk register, risk detail report, POA&M).

**Practitioners** focus on implementing the target state and measuring changes in operational risk to help plan, carry out, and monitor specific cybersecurity activities. As controls are implemented to manage risk at an acceptable level, practitioners provide managers and executives with the information (e.g., key performance indicators, key risk indicators) they need to understand the organization's cybersecurity posture, make informed decisions, and maintain or adjust the risk strategy accordingly. Executives can also combine this cybersecurity risk data with information about other types of risk from across the organization. Updates to expectations and priorities are included in updated Organizational Profiles as the cycle repeats.

### 5.2. Improving Integration with Other Risk Management Programs

Every organization faces numerous types of ICT risk (e.g., privacy, supply chain, artificial intelligence) and may use frameworks and management tools that are specific to each risk. Some organizations integrate ICT and all other risk management efforts at a high level by using ERM, while others keep the efforts separate to ensure adequate attention on each. Small organizations by their nature may monitor risk at the enterprise level, while larger companies may maintain separate risk management efforts integrated into the ERM.

Organizations can employ an ERM approach to balance a *portfolio* of risk considerations, including cybersecurity, and make informed decisions. Executives receive significant input about current and planned risk activities as they integrate governance and risk strategies with results from previous uses of the CSF. The CSF helps organizations to translate their terminology for cybersecurity and cybersecurity risk management into general risk management language that executives will understand.

NIST resources that describe the mutual relationship between cybersecurity risk management and ERM include:

- *NIST Cybersecurity Framework 2.0 – Enterprise Risk Management Quick-Start Guide*
- NIST Interagency Report (IR) 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*
- IR 8286A, *Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management*
- IR 8286B, *Prioritizing Cybersecurity Risk for Enterprise Risk Management*
- IR 8286C, *Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight*
- IR 8286D, *Using Business Impact Analysis to Inform Risk Prioritization and Response*
- SP 800-221, *Enterprise Impact of Information and Communications Technology Risk: Governing and Managing ICT Risk Programs Within an Enterprise Risk Portfolio*
- SP 800-221A, *Information and Communications Technology (ICT) Risk Outcomes: Integrating ICT Risk Management Programs with the Enterprise Risk Portfolio*

An organization may also find the CSF beneficial for integrating cybersecurity risk management with individual ICT risk management programs, such as:

- **Cybersecurity risk management and assessment:** The CSF can be integrated with established cybersecurity risk management and assessment programs, such as SP 800-37, *Risk Management Framework for Information Systems and Organizations*, and SP 800-30, *Guide for Conducting Risk Assessments* from the NIST Risk Management Framework (RMF). For an organization using the NIST RMF and its suite of publications, the CSF can be used to complement the RMF's approach to selecting and prioritizing controls from SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*.
- **Privacy risks:** While cybersecurity and privacy are independent disciplines, their objectives overlap in certain circumstances, as illustrated in Fig. 6.

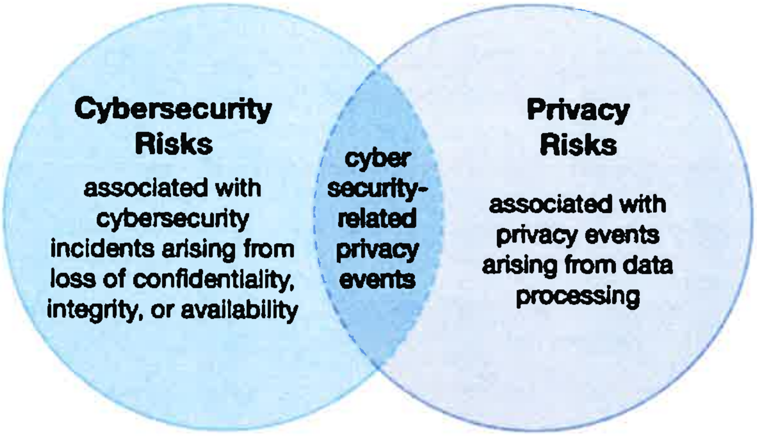

Cybersecurity Risks
associated with cybersecurity incidents arising from loss of confidentiality, integrity, or availability
cyber security-related privacy events
Privacy Risks
associated with privacy events arising from data processing

**Fig. 6. Cybersecurity and privacy risk relationship**

Cybersecurity risk management is essential for addressing privacy risks related to the loss of the confidentiality, integrity, and availability of individuals' data. For example, data breaches could lead to identity theft. However, privacy risks can also arise by means that are unrelated to cybersecurity incidents.

An organization processes data to achieve mission or business purposes, which can sometimes give rise to *privacy events* whereby individuals may experience problems as a result of the data processing. These problems can be expressed in various ways, but NIST describes them as ranging from dignity-type effects (e.g., embarrassment or stigma) to more tangible harms (e.g., discrimination, economic loss, or physical harm). The NIST Privacy Framework and Cybersecurity Framework can be used together to address the different aspects of cybersecurity and privacy risks. Additionally, NIST's Privacy Risk Assessment Methodology (PRAM) has a catalog of example problems for use in privacy risk assessments.

- **Supply chain risks:** An organization can use the CSF to foster cybersecurity risk oversight and communications with stakeholders across supply chains. All types of technology rely on a complex, globally distributed, extensive, and interconnected supply chain ecosystem with geographically diverse routes and multiple levels of outsourcing. This ecosystem is composed of public- and private-sector entities (e.g., acquirers, suppliers, developers, system integrators, external system service providers, and other technology-related service providers) that interact to research, develop, design, manufacture, acquire, deliver, integrate, operate, maintain, dispose of, and otherwise utilize or manage technology products and services. These interactions are shaped and influenced by technologies, laws, policies, procedures, and practices.

  Given the complex and interconnected relationships in this ecosystem, supply chain risk management (SCRM) is critical for organizations. Cybersecurity SCRM (C-SCRM) is a systematic process for managing exposure to cybersecurity risk throughout supply chains and developing appropriate response strategies, policies, processes, and procedures. The Subcategories within the CSF C-SCRM Category [GV.SC] provide a connection between outcomes that focus purely on cybersecurity and those that focus on C-SCRM. SP 800-161r1 (Revision 1), *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, provides in-depth information on C-SCRM.

- **Risks from emerging technologies:** As new technologies and new applications of technology become available, new risks become clear. A contemporary example is artificial intelligence (AI), which has cybersecurity and privacy risks, as well as many other types of risk. The NIST Artificial Intelligence Risk Management Framework (AI RMF) was developed to help address these risks. Treating AI risks alongside other enterprise risks (e.g., financial, cybersecurity, reputational, and privacy) will yield a more integrated outcome and organizational efficiencies. Cybersecurity and privacy risk management considerations and approaches are applicable to the design, development, deployment, evaluation, and use of AI systems. The AI RMF Core uses Functions, Categories, and Subcategories to describe AI outcomes and help manage risks related to AI.

## Appendix A. CSF Core

This appendix describes the Functions, Categories, and Subcategories of the CSF Core. Table 1 lists the CSF 2.0 Core Function and Category names and unique alphabetic identifiers. Each Function name in the table is linked to its portion of the appendix. The order of Functions, Categories, and Subcategories of the Core is not alphabetical; it is intended to resonate most with those charged with operationalizing risk management within an organization. The numbering of the Subcategories is intentionally not sequential; gaps in numbering indicate CSF 1.1 Subcategories that were relocated in CSF 2.0.

**Table 1. CSF 2.0 Core Function and Category names and identifiers**

| Function | Category | Category Identifier |
|---|---|---|
| Govern (GV) | Organizational Context | GV.OC |
| | Risk Management Strategy | GV.RM |
| | Roles, Responsibilities, and Authorities | GV.RR |
| | Policy | GV.PO |
| | Oversight | GV.OV |
| | Cybersecurity Supply Chain Risk Management | GV.SC |
| Identify (ID) | Asset Management | ID.AM |
| | Risk Assessment | ID.RA |
| | Improvement | ID.IM |
| Protect (PR) | Identity Management, Authentication, and Access Control | PR.AA |
| | Awareness and Training | PR.AT |
| | Data Security | PR.DS |
| | Platform Security | PR.PS |
| | Technology Infrastructure Resilience | PR.IR |
| Detect (DE) | Continuous Monitoring | DE.CM |
| | Adverse Event Analysis | DE.AE |
| Respond (RS) | Incident Management | RS.MA |
| | Incident Analysis | RS.AN |
| | Incident Response Reporting and Communication | RS.CO |
| | Incident Mitigation | RS.MI |
| Recover (RC) | Incident Recovery Plan Execution | RC.RP |
| | Incident Recovery Communication | RC.CO |

The CSF Core, Informative References, and Implementation Examples are available on the CSF 2.0 website and through the CSF 2.0 Reference Tool, which allows users to explore them and export them in human- and machine-readable formats. The CSF 2.0 Core is also available in a legacy format similar to that of CSF 1.1.

**GOVERN (GV):** The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored

- **Organizational Context (GV.OC):** The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood
  - **GV.OC-01:** The organizational mission is understood and informs cybersecurity risk management
  - **GV.OC-02:** Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered
  - **GV.OC-03:** Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed
  - **GV.OC-04:** Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated
  - **GV.OC-05:** Outcomes, capabilities, and services that the organization depends on are understood and communicated
- **Risk Management Strategy (GV.RM):** The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions
  - **GV.RM-01:** Risk management objectives are established and agreed to by organizational stakeholders
  - **GV.RM-02:** Risk appetite and risk tolerance statements are established, communicated, and maintained
  - **GV.RM-03:** Cybersecurity risk management activities and outcomes are included in enterprise risk management processes
  - **GV.RM-04:** Strategic direction that describes appropriate risk response options is established and communicated
  - **GV.RM-05:** Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties
  - **GV.RM-06:** A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated
  - **GV.RM-07:** Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions

- **Roles, Responsibilities, and Authorities (GV.RR):** Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated
  - **GV.RR-01:** Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving
  - **GV.RR-02:** Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced
  - **GV.RR-03:** Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies
  - **GV.RR-04:** Cybersecurity is included in human resources practices
- **Policy (GV.PO):** Organizational cybersecurity policy is established, communicated, and enforced
  - **GV.PO-01:** Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced
  - **GV.PO-02:** Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission
- **Oversight (GV.OV):** Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy
  - **GV.OV-01:** Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction
  - **GV.OV-02:** The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks
  - **GV.OV-03:** Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed
- **Cybersecurity Supply Chain Risk Management (GV.SC):** Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders
  - **GV.SC-01:** A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders
  - **GV.SC-02:** Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally
  - **GV.SC-03:** Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes
  - **GV.SC-04:** Suppliers are known and prioritized by criticality

- **GV.SC-05:** Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties
- **GV.SC-06:** Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships
- **GV.SC-07:** The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship
- **GV.SC-08:** Relevant suppliers and other third parties are included in incident planning, response, and recovery activities
- **GV.SC-09:** Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle
- **GV.SC-10:** Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement

**IDENTIFY (ID):** The organization's current cybersecurity risks are understood

- **Asset Management (ID.AM):** Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy
  - **ID.AM-01:** Inventories of hardware managed by the organization are maintained
  - **ID.AM-02:** Inventories of software, services, and systems managed by the organization are maintained
  - **ID.AM-03:** Representations of the organization's authorized network communication and internal and external network data flows are maintained
  - **ID.AM-04:** Inventories of services provided by suppliers are maintained
  - **ID.AM-05:** Assets are prioritized based on classification, criticality, resources, and impact on the mission
  - **ID.AM-07:** Inventories of data and corresponding metadata for designated data types are maintained
  - **ID.AM-08:** Systems, hardware, software, services, and data are managed throughout their life cycles
- **Risk Assessment (ID.RA):** The cybersecurity risk to the organization, assets, and individuals is understood by the organization
  - **ID.RA-01:** Vulnerabilities in assets are identified, validated, and recorded

  - **ID.RA-02:** Cyber threat intelligence is received from information sharing forums and sources
  - **ID.RA-03:** Internal and external threats to the organization are identified and recorded
  - **ID.RA-04:** Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded
  - **ID.RA-05:** Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization
  - **ID.RA-06:** Risk responses are chosen, prioritized, planned, tracked, and communicated
  - **ID.RA-07:** Changes and exceptions are managed, assessed for risk impact, recorded, and tracked
  - **ID.RA-08:** Processes for receiving, analyzing, and responding to vulnerability disclosures are established
  - **ID.RA-09:** The authenticity and integrity of hardware and software are assessed prior to acquisition and use
  - **ID.RA-10:** Critical suppliers are assessed prior to acquisition

- **Improvement (ID.IM):** Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions
  - **ID.IM-01:** Improvements are identified from evaluations
  - **ID.IM-02:** Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties
  - **ID.IM-03:** Improvements are identified from execution of operational processes, procedures, and activities
  - **ID.IM-04:** Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved

**PROTECT (PR):** Safeguards to manage the organization's cybersecurity risks are used

- **Identity Management, Authentication, and Access Control (PR.AA):** Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access
  - **PR.AA-01:** Identities and credentials for authorized users, services, and hardware are managed by the organization
  - **PR.AA-02:** Identities are proofed and bound to credentials based on the context of interactions
  - **PR.AA-03:** Users, services, and hardware are authenticated
  - **PR.AA-04:** Identity assertions are protected, conveyed, and verified

  - **PR.AA-05:** Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties
  - **PR.AA-06:** Physical access to assets is managed, monitored, and enforced commensurate with risk

- **Awareness and Training (PR.AT):** The organization's personnel are provided with cybersecurity awareness and training so that they can perform their cybersecurity-related tasks
  - **PR.AT-01:** Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind
  - **PR.AT-02:** Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind

- **Data Security (PR.DS):** Data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information
  - **PR.DS-01:** The confidentiality, integrity, and availability of data-at-rest are protected
  - **PR.DS-02:** The confidentiality, integrity, and availability of data-in-transit are protected
  - **PR.DS-10:** The confidentiality, integrity, and availability of data-in-use are protected
  - **PR.DS-11:** Backups of data are created, protected, maintained, and tested

- **Platform Security (PR.PS):** The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability
  - **PR.PS-01:** Configuration management practices are established and applied
  - **PR.PS-02:** Software is maintained, replaced, and removed commensurate with risk
  - **PR.PS-03:** Hardware is maintained, replaced, and removed commensurate with risk
  - **PR.PS-04:** Log records are generated and made available for continuous monitoring
  - **PR.PS-05:** Installation and execution of unauthorized software are prevented
  - **PR.PS-06:** Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle

- **Technology Infrastructure Resilience (PR.IR):** Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience
  - **PR.IR-01:** Networks and environments are protected from unauthorized logical access and usage

  - **PR.IR-02:** The organization's technology assets are protected from environmental threats
  - **PR.IR-03:** Mechanisms are implemented to achieve resilience requirements in normal and adverse situations
  - **PR.IR-04:** Adequate resource capacity to ensure availability is maintained

**DETECT (DE):** Possible cybersecurity attacks and compromises are found and analyzed

- **Continuous Monitoring (DE.CM):** Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events
  - **DE.CM-01:** Networks and network services are monitored to find potentially adverse events
  - **DE.CM-02:** The physical environment is monitored to find potentially adverse events
  - **DE.CM-03:** Personnel activity and technology usage are monitored to find potentially adverse events
  - **DE.CM-06:** External service provider activities and services are monitored to find potentially adverse events
  - **DE.CM-09:** Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events
- **Adverse Event Analysis (DE.AE):** Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents
  - **DE.AE-02:** Potentially adverse events are analyzed to better understand associated activities
  - **DE.AE-03:** Information is correlated from multiple sources
  - **DE.AE-04:** The estimated impact and scope of adverse events are understood
  - **DE.AE-06:** Information on adverse events is provided to authorized staff and tools
  - **DE.AE-07:** Cyber threat intelligence and other contextual information are integrated into the analysis
  - **DE.AE-08:** Incidents are declared when adverse events meet the defined incident criteria

**RESPOND (RS):** Actions regarding a detected cybersecurity incident are taken

- **Incident Management (RS.MA):** Responses to detected cybersecurity incidents are managed
    - **RS.MA-01:** The incident response plan is executed in coordination with relevant third parties once an incident is declared
    - **RS.MA-02:** Incident reports are triaged and validated
    - **RS.MA-03:** Incidents are categorized and prioritized
    - **RS.MA-04:** Incidents are escalated or elevated as needed
    - **RS.MA-05:** The criteria for initiating incident recovery are applied
- **Incident Analysis (RS.AN):** Investigations are conducted to ensure effective response and support forensics and recovery activities
    - **RS.AN-03:** Analysis is performed to establish what has taken place during an incident and the root cause of the incident
    - **RS.AN-06:** Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved
    - **RS.AN-07:** Incident data and metadata are collected, and their integrity and provenance are preserved
    - **RS.AN-08:** An incident's magnitude is estimated and validated
- **Incident Response Reporting and Communication (RS.CO):** Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies
    - **RS.CO-02:** Internal and external stakeholders are notified of incidents
    - **RS.CO-03:** Information is shared with designated internal and external stakeholders
- **Incident Mitigation (RS.MI):** Activities are performed to prevent expansion of an event and mitigate its effects
    - **RS.MI-01:** Incidents are contained
    - **RS.MI-02:** Incidents are eradicated

**RECOVER (RC):** Assets and operations affected by a cybersecurity incident are restored

- **Incident Recovery Plan Execution (RC.RP):** Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents
    - **RC.RP-01:** The recovery portion of the incident response plan is executed once initiated from the incident response process

  - **RC.RP-02:** Recovery actions are selected, scoped, prioritized, and performed
  - **RC.RP-03:** The integrity of backups and other restoration assets is verified before using them for restoration
  - **RC.RP-04:** Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms
  - **RC.RP-05:** The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed
  - **RC.RP-06:** The end of incident recovery is declared based on criteria, and incident-related documentation is completed

- **Incident Recovery Communication (RC.CO):** Restoration activities are coordinated with internal and external parties
  - **RC.CO-03:** Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders
  - **RC.CO-04:** Public updates on incident recovery are shared using approved methods and messaging

## Appendix B. CSF Tiers

Table 2 contains a notional illustration of the CSF Tiers discussed in Sec. 3. The Tiers characterize the rigor of an organization's cybersecurity risk governance practices (GOVERN) and cybersecurity risk management practices (IDENTIFY, PROTECT, DETECT, RESPOND, and RECOVER).

**Table 2. Notional Illustration of the CSF Tiers**

| Tier | Cybersecurity Risk Governance | Cybersecurity Risk Management |
|---|---|---|
| Tier 1: Partial | Application of the organizational cybersecurity risk strategy is managed in an ad hoc manner.<br>Prioritization is ad hoc and not formally based on objectives or threat environment. | There is limited awareness of cybersecurity risks at the organizational level.<br>The organization implements cybersecurity risk management on an irregular, case-by-case basis.<br>The organization may not have processes that enable cybersecurity information to be shared within the organization.<br>The organization is generally unaware of the cybersecurity risks associated with its suppliers and the products and services it acquires and uses. |
| Tier 2: Risk Informed | Risk management practices are approved by management but may not be established as organization-wide policy.<br>The prioritization of cybersecurity activities and protection needs is directly informed by organizational risk objectives, the threat environment, or business/mission requirements. | There is an awareness of cybersecurity risks at the organizational level, but an organization-wide approach to managing cybersecurity risks has not been established.<br>Consideration of cybersecurity in organizational objectives and programs may occur at some but not all levels of the organization. Cyber risk assessment of organizational and external assets occurs but is not typically repeatable or reoccurring.<br>Cybersecurity information is shared within the organization on an informal basis.<br>The organization is aware of the cybersecurity risks associated with its suppliers and the products and services it acquires and uses, but it does not act consistently or formally in response to those risks. |
| Tier 3: Repeatable | The organization's risk management practices are formally approved and expressed as policy.<br>Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed.<br>Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements, threats, and technological landscape. | There is an organization-wide approach to managing cybersecurity risks. Cybersecurity information is routinely shared throughout the organization.<br>Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities.<br>The organization consistently and accurately monitors the cybersecurity risks of assets. Senior cybersecurity and non-cybersecurity executives communicate regularly regarding cybersecurity risks. Executives ensure that cybersecurity is considered through all lines of operation in the organization. |

| Tier | Cybersecurity Risk Governance | Cybersecurity Risk Management |
|---|---|---|
| | | The organization risk strategy is informed by the cybersecurity risks associated with its suppliers and the products and services it acquires and uses. Personnel formally act upon those risks through mechanisms such as written agreements to communicate baseline requirements, governance structures (e.g., risk councils), and policy implementation and monitoring. These actions are implemented consistently and as intended and are continuously monitored and reviewed. |
| Tier 4: Adaptive | There is an organization-wide approach to managing cybersecurity risks that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. The relationship between cybersecurity risks and organizational objectives is clearly understood and considered when making decisions. Executives monitor cybersecurity risks in the same context as financial and other organizational risks. The organizational budget is based on an understanding of the current and predicted risk environment and risk tolerance. Business units implement executive vision and analyze system-level risks in the context of the organizational risk tolerances.<br>Cybersecurity risk management is part of the organizational culture. It evolves from an awareness of previous activities and continuous awareness of activities on organizational systems and networks. The organization can quickly and efficiently account for changes to business/mission objectives in how risk is approached and communicated. | The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators. Through a process of continuous improvement that incorporates advanced cybersecurity technologies and practices, the organization actively adapts to a changing technological landscape and responds in a timely and effective manner to evolving, sophisticated threats.<br>The organization uses real-time or near real-time information to understand and consistently act upon the cybersecurity risks associated with its suppliers and the products and services it acquires and uses.<br>Cybersecurity information is constantly shared throughout the organization and with authorized third parties. |

## Appendix C. Glossary

**CSF Category**
A group of related cybersecurity outcomes that collectively comprise a CSF Function.

**CSF Community Profile**
A baseline of CSF outcomes that is created and published to address shared interests and goals among a number of organizations. A Community Profile is typically developed for a particular sector, subsector, technology, threat type, or other use case. An organization can use a Community Profile as the basis for its own Target Profile.

**CSF Core**
A taxonomy of high-level cybersecurity outcomes that can help any organization manage its cybersecurity risks. Its components are a hierarchy of Functions, Categories, and Subcategories that detail each outcome.

**CSF Current Profile**
A part of an Organizational Profile that specifies the Core outcomes that an organization is currently achieving (or attempting to achieve) and characterizes how or to what extent each outcome is being achieved.

**CSF Function**
The highest level of organization for cybersecurity outcomes. There are six CSF Functions: Govern, Identify, Protect, Detect, Respond, and Recover.

**CSF Implementation Example**
A concise, action-oriented, notional illustration of a way to help achieve a CSF Core outcome.

**CSF Informative Reference**
A mapping that indicates a relationship between a CSF Core outcome and an existing standard, guideline, regulation, or other content.

**CSF Organizational Profile**
A mechanism for describing an organization's current and/or target cybersecurity posture in terms of the CSF Core's outcomes.

**CSF Quick Start Guide**
A supplementary resource that gives brief, actionable guidance on specific CSF-related topics.

**CSF Subcategory**
A group of more specific outcomes of technical and management cybersecurity activities that comprise a CSF Category.

**CSF Target Profile**
A part of an Organizational Profile that specifies the desired Core outcomes that an organization has selected and prioritized for achieving its cybersecurity risk management objectives.

**CSF Tier**
A characterization of the rigor of an organization's cybersecurity risk governance and management practices. There are four Tiers: Partial (Tier 1), Risk Informed (Tier 2), Repeatable (Tier 3), and Adaptive (Tier 4).

Certain commercial equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

### NIST Technical Series Policies

Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

### How to Cite this NIST Technical Series Publication:

National Institute of Standards and Technology (2024) The NIST Cybersecurity Framework (CSF) 2.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 29. https://doi.org/10.6028/NIST.CSWP.29

### Contact Information

cyberframework@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

**All comments are subject to release under the Freedom of Information Act (FOIA).**

Item #8

## Memorandum

**From:** Terry O'Neil, Town Management Consultant

**To:** Town Council and Mayor

**Date:** December 5, 2024

**Re:** Martin County request for a letter in support of its efforts to secure grant funding to build a Brightline passenger rail station in Downtown Stuart

---

Martin County is requesting a letter supporting its efforts to obtain grants to help fund a Brightline passenger rail station on Flagler Avenue in Downtown Stuart. Please see the attached correspondence from Assistant County Administrator, George Stokus.

**Background:**

The Florida East Coast Railroad's recent addition of a second track -- intended to accommodate both enhanced freight traffic and passenger rail services -- has been a matter of local controversy for several years. Over most of that time, Martin County government (and others) have vigorously opposed the railroad's expansion. Then, in November 2018, with most of its legal options exhausted, the County entered into a settlement agreement that included a commitment by the railroad to build a passenger station on the Treasure Coast, subject to a number of conditions. Brightline has established active stations in Miami, Aventura, Fort Lauderdale, Boca Raton, West Palm Beach and Orlando.

In August, 2024, a newly-constituted Stuart City Commission, which for many years had advocated for a downtown station, both through its comprehensive plan policies, as well as a more recent three-party (City/County/RR) agreement, withdrew its support citing exorbitant local (city) costs for the project, as well as concerns about overdevelopment. Since then, the Board of County Commissioners has, on its own, chosen to pursue construction of a Brightline station on property it owns on Flagler Avenue. The site is the same location previously agreed upon in the now-dissolved three-party City/County/RR agreement.

**Recommendation:**

The topic of building a Brightline station in downtown Stuart remains controversial. Regarding the County's request, staff suggests that the Council invite public comment and then exercise its best judgment on behalf of the Town. If the proposed letter is approved, staff has taken the liberty of adding language that reiterates the Town's support for local quiet zones and other noise mitigation techniques, including access to any grant funds necessary to help bring them about.

**Town Clerk**

**From:** Terrance O'Neil <terrancewoneil@gmail.com>
**Sent:** Thursday, November 21, 2024 8:42 PM
**To:** Town Clerk
**Cc:** Permits; Karen Ostrand; Gemma Torcivia; Paul Nicoletti; George Stokus; Don Donaldson
**Subject:** Fwd: Request for Support Letter - FRA Grant for Brightline Station in Martin County
**Attachments:** Martin County Support Letter.docx

**Follow Up Flag:** Flag for follow up
**Flag Status:** Flagged

To: Kim Stanton, Town Clerk

Please share this email and attachment from Martin County Assistant Administrator, George Stokus, with our Mayor, current council members, and soon-to-be seated council members who will be sworn in at our next regularly scheduled Council meeting on December 9, 2024. Unfortunately, notwithstanding Mr. Stokus's request that we consider and provide a letter of support for a Stuart/Martin County train station by December 2, 2024, we cannot do so until the Council next meets. Please plan on adding this item to our December 9 agenda unless George tells us it's too late to matter.

Thanks,

Terry

Sent from my iPhone

Begin forwarded message:

> **From:** George Stokus <gstokus@martin.fl.us>
> **Date:** November 21, 2024 at 5:49:45 PM EST
> **Cc:** Carolyn Schmidt <carolyns@martin.fl.us>, George Stokus <gstokus@martin.fl.us>
> **Subject: Request for Support Letter - FRA Grant for Brightline Station in Martin County**
>
> Hello All,
>
> I hope this email finds you well. I am writing to request your support for the Federal Railroad Administration (FRA) grant application for a Brightline station in Martin County.
>
> As you may be aware, Brightline has selected Stuart, Florida as the site for its next intercity passenger rail station. This exciting development promises to bring significant benefits to our community, including improved connectivity and economic growth. Attached is a template letter, but we encourage to make this letter your own. Your support letter would greatly strengthen our grant application.

It should highlight:

1. The positive impact of the station on local transportation
2. Potential economic benefits for the region
3. The broad community support for this project

The proposed station location is 500 S.E. Flagler Avenue in downtown Stuart, with groundbreaking expected in early 2026 and completion in early 2028.

We would greatly appreciate your support in this endeavor. Please let me know if you need any additional information to draft the letter. Please send your signed letter to carolyns@martin.fl.us by 12:00 PM on 12/2/24. If you know a businesses that will benefit from the construction of a Brightline Station, please forward this email and encourage them to write a letter of support to be included in our application.

Thank you for your time and consideration.

Respectfully,

George M. Stokus, A.A.E.
Assistant County Administrator
Martin County Board of County Commissioners

(772) 221-2352
2401 SE Monterey Rd.
Stuart FL, 34994

This document may be reproduced upon request in an alternative format by contacting the County ADA Coordinator (772) 320-3131, the County Administration Office (772) 288-5400, Florida Relay 711, or by completing our accessibility feedback form at www.martin.fl.us/accessibility-feedback

***The comments and opinions expressed herein are those of the author of this message and may not reflect the policies of the Martin County Board of County Commissioners. Under Florida Law, email addresses are public records. If you do not want your email address released in response to a public records request do not send electronic mail to this entity. Instead, contact this office by phone or in writing.***

[YOUR ORGANIZATION'S LETTERHEAD]
[DATE]

Secretary
U.S. Department of Transportation
1200 New Jersey Avenue, SE
Washington, DC 20590

Administrator
Federal Railroad Administration
1200 New Jersey Avenue, SE
Washington, DC 20590

**Re: Strong Support for Martin County's Proposed Rail Station Construction**

Dear Secretary and Administrator:

I write on behalf of [ORGANIZATION NAME] to convey our strong support for Martin County's Federal-State Partnership for Intercity Passenger Rail grant application to the Federal Railroad Administration. Martin County seeks funding to support the final design and construction of a high-speed rail station. FRA assistance will help Martin County to construct a train infrastructure that reduces highway congestion and promotes economic development.

In 2018, the privately-owned Brightline intercity passenger rail service began high-speed train operations between West Palm Beach and Miami, traveling a 70-mile route in 75 minutes. Last year, Brightline expanded service north to Orlando, connecting Florida's beaches to America's theme park capital. A future extension to Tampa is also planned. Brightline's high-speed trains began moving through Martin County in September 2023. Sixteen daily roundtrips are planned between Orlando and Miami. Working with Brightline, Martin County seeks to develop a high-speed rail station in the community to support intercity travel for residents and visitors.

[ORGANIZATION NAME] supports Martin County's effort to develop a high-speed rail station because [write a line or two about your particular interests in the project; describe how the train station will support jobs, growth, and equity in the area].

Please give the highest consideration to Martin County's application for FRA Federal-State Partnership for Intercity Passenger Rail funding. Thank you very much.

Sincerely,

[NAME, TITLE, ORGANIZATION]

**Town of Ocean Breeze**

December 9, 2024

Secretary
U.S. Department of Transportation
1200 New Jersey Avenue, SE
Washington, DC 20590

Administrator
Federal Railroad Administration
1200 New Jersey Avenue, SE
Washington, DC 20590

**Re: Strong Support for Martin County's Proposed Rail Station Construction**

Dear Secretary and Administrator:

I write on behalf of the Town of Ocean Breeze to convey our strong support for Martin County's Federal-State Partnership for Intercity Passenger Rail grant application to the Federal Railroad Administration. Martin County seeks funding to support the final design and construction of a high-speed rail station. FRA assistance will help Martin County to construct a train infrastructure that reduces highway congestion and promotes economic development.

In 2018, the privately-owned Brightline intercity passenger rail service began high-speed train operations between West Palm Beach and Miami, traveling a 70-mile route in 75 minutes. Last year, Brightline expanded service north to Orlando, connecting Florida's beaches to America's theme park capital. A future extension to Tampa is also planned. Brightline's high-speed trains began moving through Martin County in September 2023. Sixteen daily roundtrips are planned between Orlando and Miami. Working with Brightline, Martin County seeks to develop a high-speed rail station in the community to support intercity travel for residents and visitors.

The Town of Ocean Breeze supports Martin County's effort to develop a high-speed rail station because the train station will support jobs and growth in the area.

Please give the highest consideration to Martin County's application for FRA Federal-State Partnership for Intercity Passenger Rail funding.

Finally, on a related matter, the Town of Ocean Breeze wishes to reiterate its support for local quiet zones, way-side horns and other noise mitigation techniques, including access to any grant funds necessary to help bring these vital improvements about.

Please see attached Resolution No. 345-2024.

Thank you very much.

Sincerely,

President

Karen M. Ostrand, Mayor

cc Martin County Board of County Commissioners
Don Donaldson, Martin County Administrator
George Stokus, Martin County Assistant Administrator
City of Stuart
Town of Jupiter Island
Village of Indiantown
Town of Sewall's Point

**BEFORE THE TOWN COUNCIL OF THE
TOWN OF OCEAN BREEZE, FLORIDA**

# RESOLUTION NO. 345-2024

**A RESOLUTION OF THE TOWN COUNCIL OF THE TOWN OF OCEAN BREEZE, FLORIDA, ENCOURAGING THE MARTIN COUNTY BOARD OF COUNTY COMMISSIONERS AND THE STUART CITY COMMISSION TO SEEK COUNTY-WIDE "QUIET ZONE" STATUS -- AS PERMITTED BY SECTION 49, PART 222 OF THE CODE OF FEDERAL REGULATIONS -- THEREBY CURTAILING INTRUSIVE TRAIN HORN NOISE STEMMING FROM INCREASED FREIGHT AND HIGH SPEED PASSENGER RAIL TRAFFIC ON THE FLORIDA EAST COAST RAILROAD (FEC) RIGHT-OF-WAY; PROVIDING FOR AN EFFECTIVE DATE AND FOR OTHER PURPOSES.**

*******

**WHEREAS,** the Florida East Coast Railroad (FEC) recently double tracked its right-of-way to accommodate ever-increasing freight traffic, as well as Brightline's high speed passenger rail service between Miami and Orlando; and

**WHEREAS,** fully seventy-five percent of Ocean Breeze residents live within a half mile of the FEC right-right-of-way and are substantially burdened by FEC/Brightline's enthusiastic use of train horns at all hours of the day and night; and

**WHEREAS,** in light of recently-completed safety improvements at several FEC railroad interesections, Martin County and the City of Stuart are strongly positioned to jointly seek county-wide "quiet zone" status, thereby benefiting Ocean Breeze, Stuart and Martin County residents alike; and

**WHEREAS,** mitigating against the negative impacts of increased railroad traffic is wholly within the Public's best interest.

**NOW, THEREFORE, THE OCEAN BREEZE TOWN COUNCIL HEREBY RESOLVES THAT:**

**SECTION 1.** The Martin County Board of County Commissioners and the Stuart City Commission are hereby encourage to jointly seek county-wide "quiet zone" status for the FEC right-of-way, including any other noise-abatement measures that may be approriate.

**SECTION 2.** This resolution shall take effect immediately upon its adoption.

**SECTION 3.** The Ocean Breeze Town Clerk is hereby directed to promtly transmit this resolution to the Martin County Board of County Commissioners, the Stuart City Commisson and to their senior staff.

**APPROVED AND ADOPTED** this 12$^{TH}$ day of February, 2024.

| | YES | NO | ABSENT |
|---|---|---|---|
| SANDY KELLEY, PRESIDENT | X | | |
| LIZ REESE, VICE-PRESIDENT | X | | |
| GINA KENT, COUNCIL MEMBER | X | | |
| KEVIN DOCHERTY, COUNCIL MEMBER | X | | |
| MICHAEL HELLER, COUNCIL MEMBER | X | | |
| MATTHEW SQUIRES, COUNCIL MEMBER | X | | |

ATTEST:

KIM STANTON
TOWN CLERK

Sandy Kelley

SANDY KELLEY
COUNCIL PRESIDENT

Nicole Laliberte

NICOLE LALIBERTE
TOWN ATTORNEY

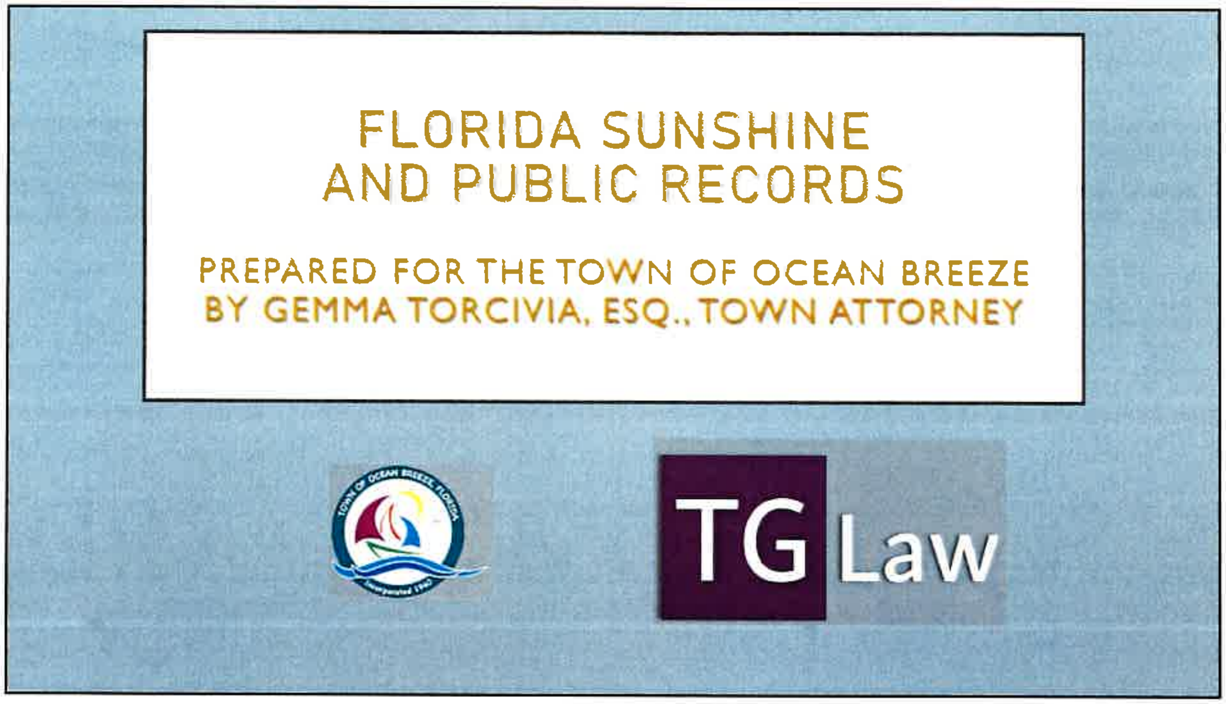
Karen M Ostrand

KAREN M. OSTRAND
MAYOR

APPROVED AS TO FORM

TOWN OF OCEAN BREEZE
Incorporated
FLORIDA

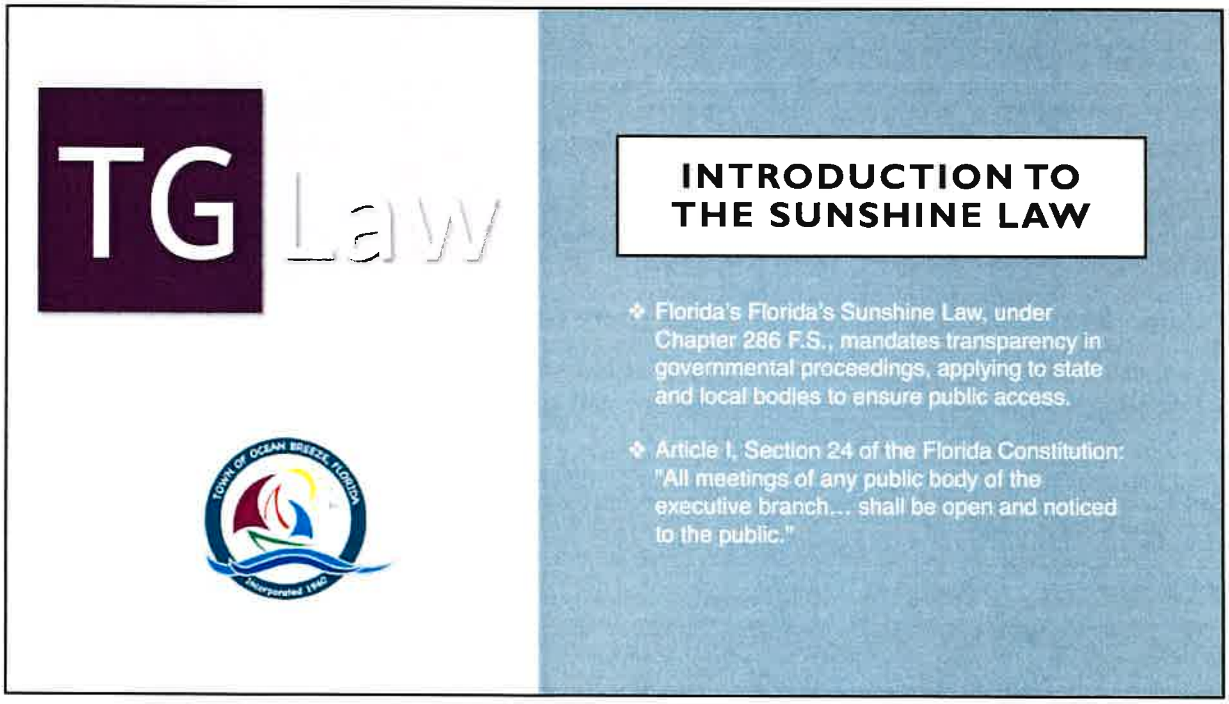
Item #12



# FLORIDA SUNSHINE AND PUBLIC RECORDS

PREPARED FOR THE TOWN OF OCEAN BREEZE
BY GEMMA TORCIVIA, ESQ., TOWN ATTORNEY

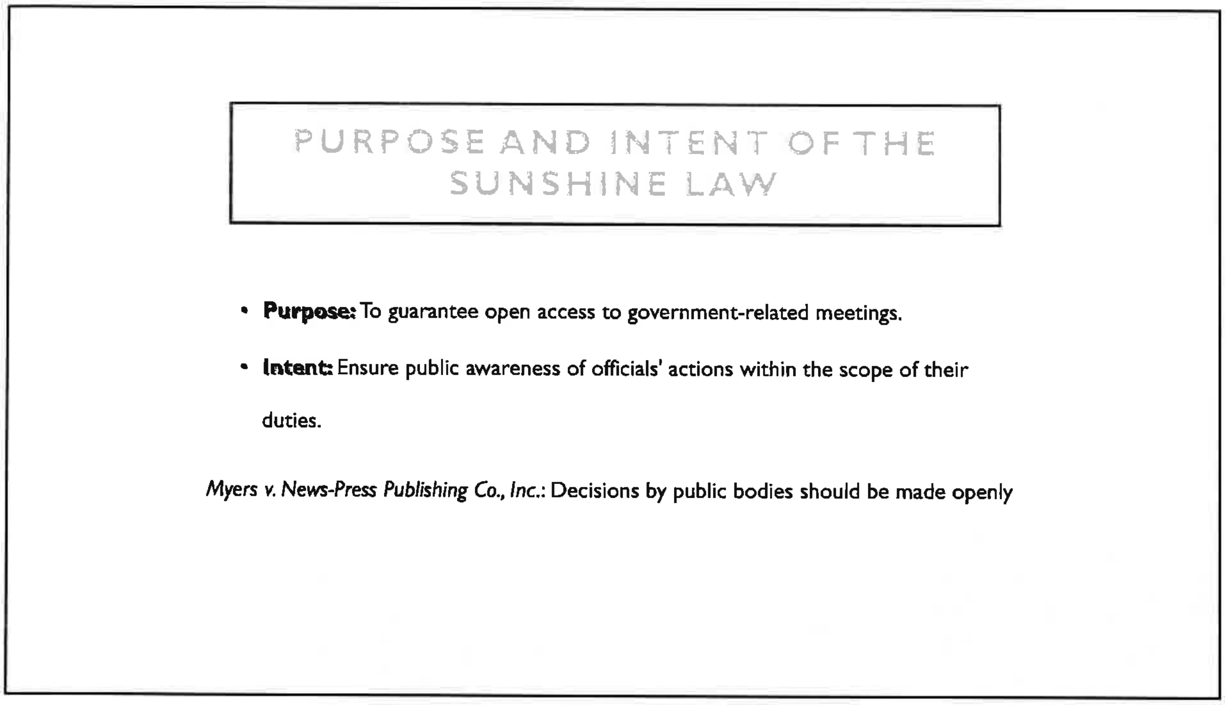
1



## INTRODUCTION TO THE SUNSHINE LAW

- Florida's Florida's Sunshine Law, under Chapter 286 F.S., mandates transparency in governmental proceedings, applying to state and local bodies to ensure public access.
- Article I, Section 24 of the Florida Constitution: "All meetings of any public body of the executive branch... shall be open and noticed to the public."

2

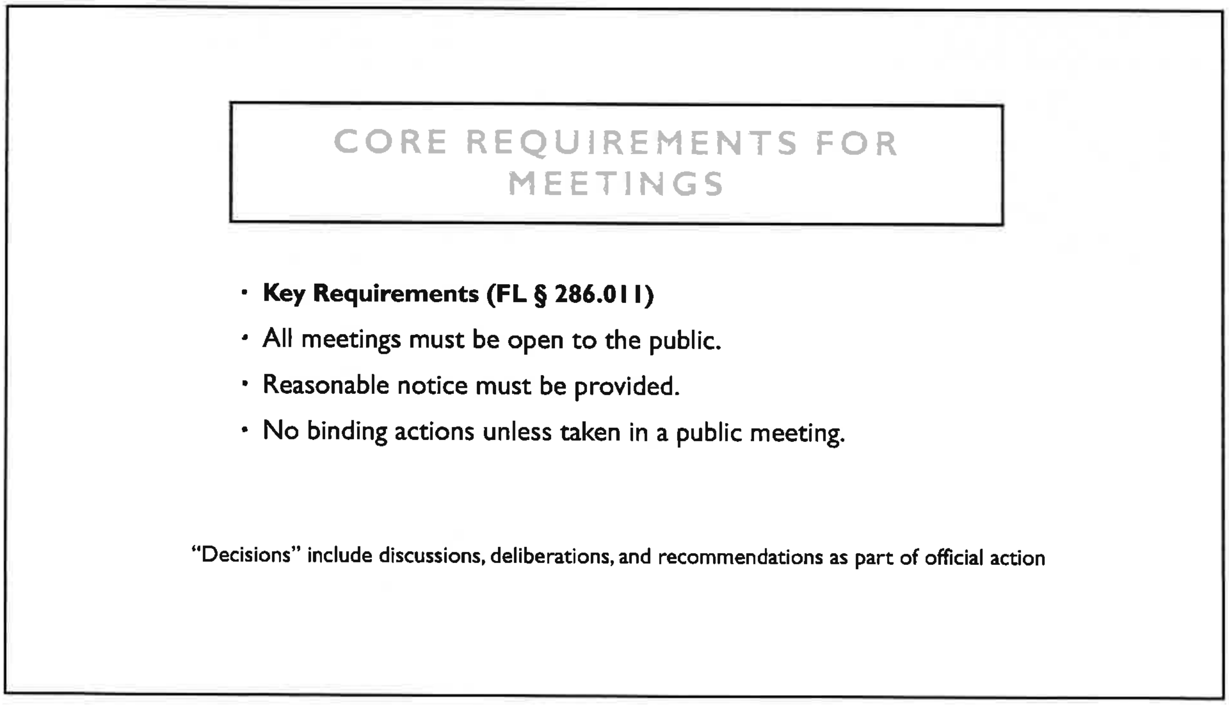


## PURPOSE AND INTENT OF THE SUNSHINE LAW

- **Purpose:** To guarantee open access to government-related meetings.
- **Intent:** Ensure public awareness of officials' actions within the scope of their duties.

*Myers v. News-Press Publishing Co., Inc.*: Decisions by public bodies should be made openly

3

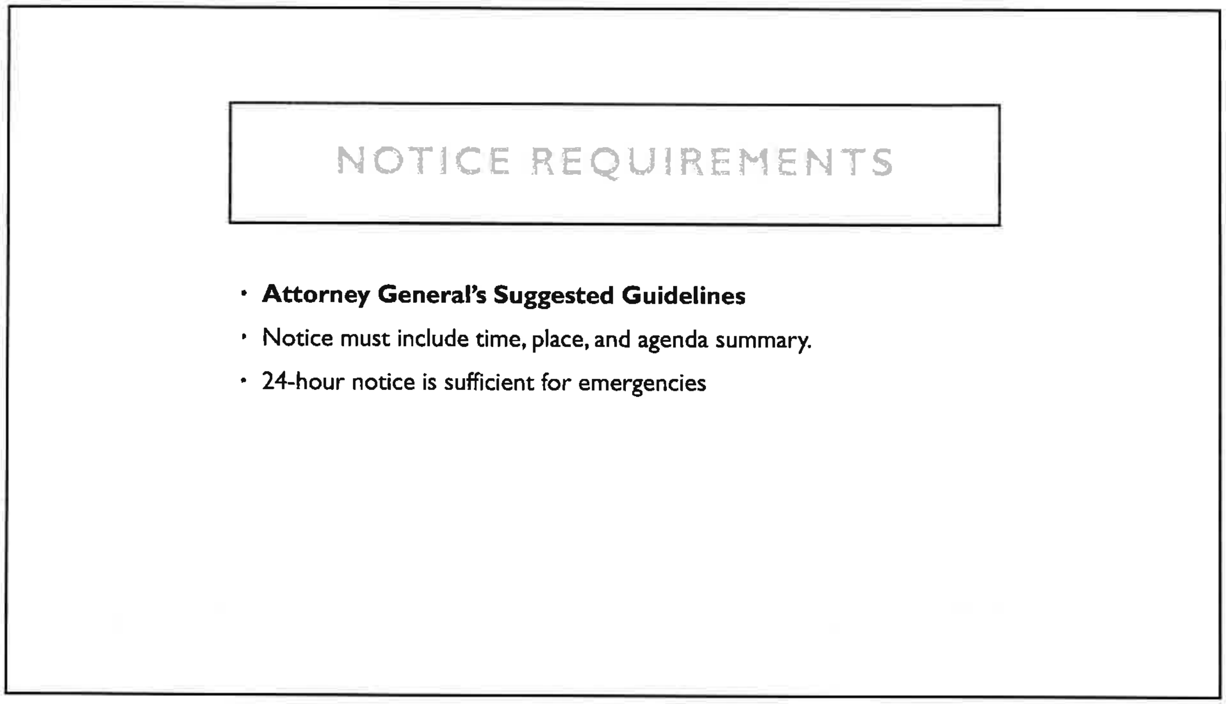


## CORE REQUIREMENTS FOR MEETINGS

- **Key Requirements (FL § 286.011)**
- All meetings must be open to the public.
- Reasonable notice must be provided.
- No binding actions unless taken in a public meeting.

"Decisions" include discussions, deliberations, and recommendations as part of official action

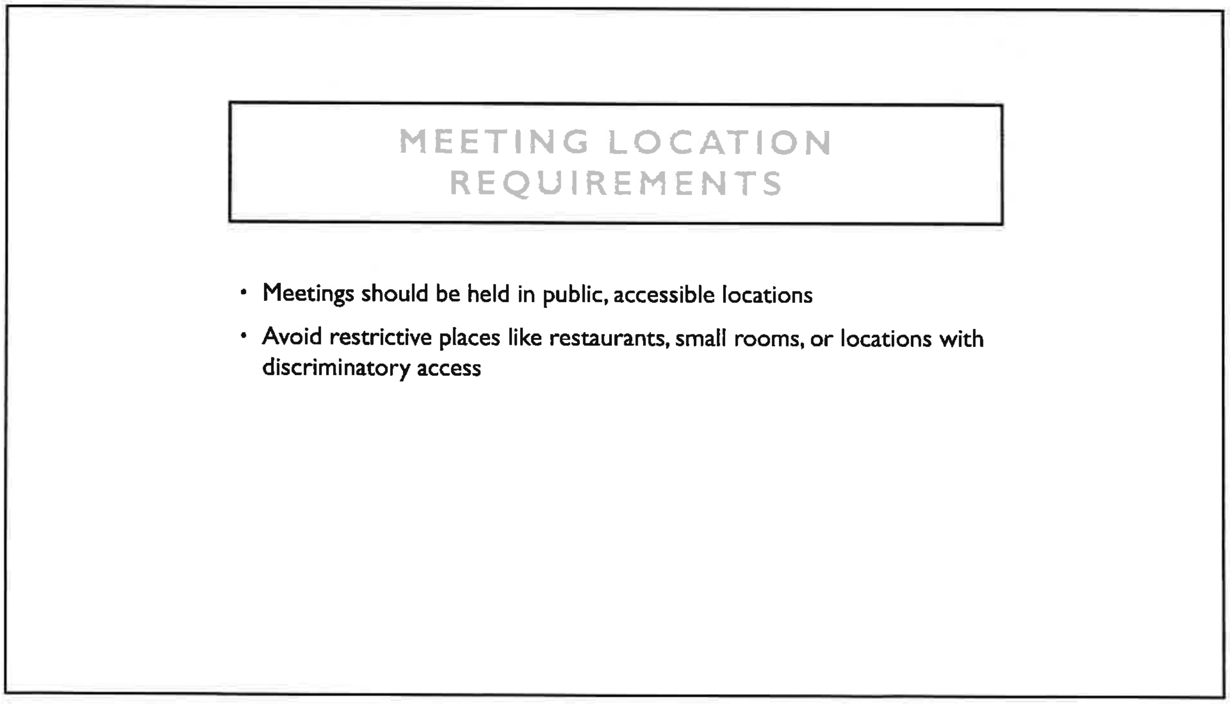
4



## NOTICE REQUIREMENTS

- **Attorney General's Suggested Guidelines**
- Notice must include time, place, and agenda summary.
- 24-hour notice is sufficient for emergencies

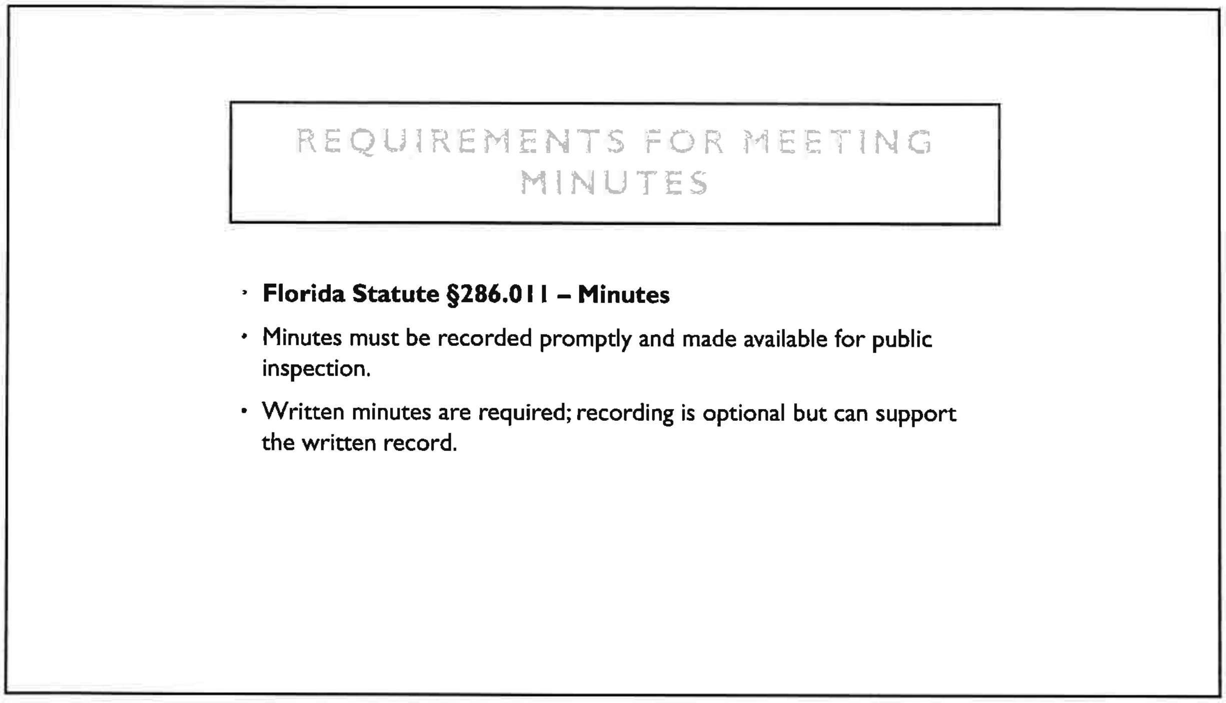
5



## MEETING LOCATION REQUIREMENTS

- Meetings should be held in public, accessible locations
- Avoid restrictive places like restaurants, small rooms, or locations with discriminatory access

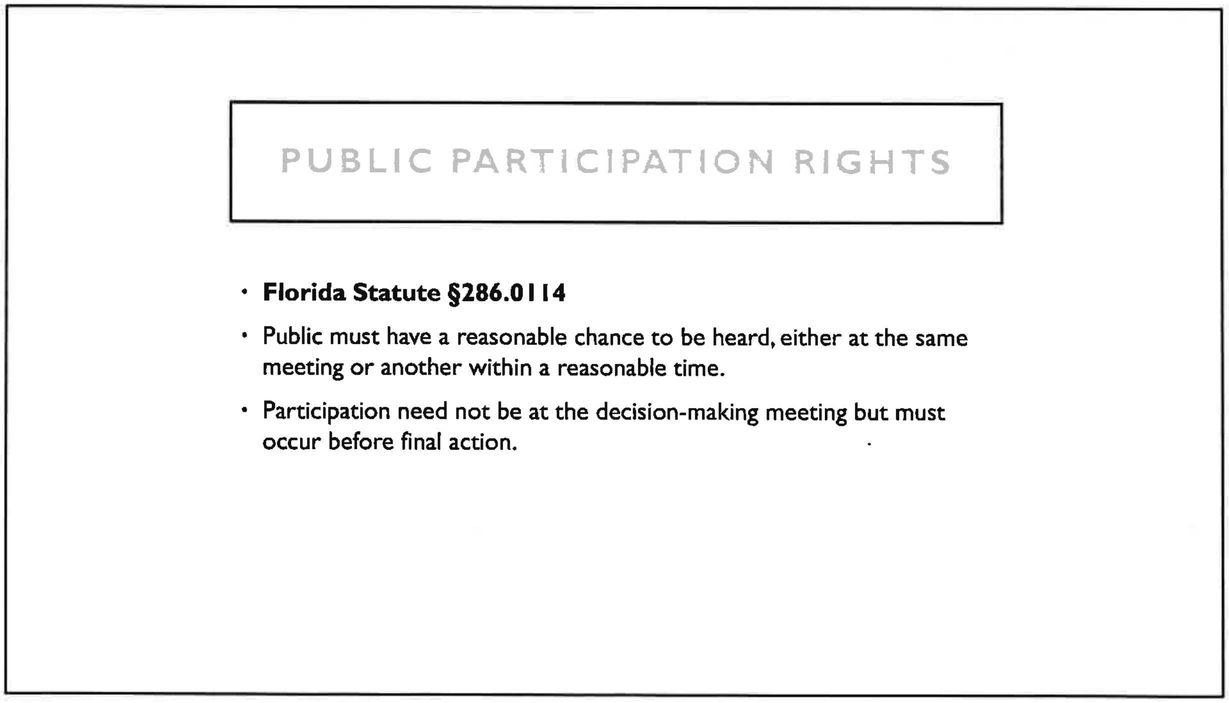
6



## REQUIREMENTS FOR MEETING MINUTES

- **Florida Statute §286.011 – Minutes**
- Minutes must be recorded promptly and made available for public inspection.
- Written minutes are required; recording is optional but can support the written record.

7



## PUBLIC PARTICIPATION RIGHTS

- **Florida Statute §286.0114**
- Public must have a reasonable chance to be heard, either at the same meeting or another within a reasonable time.
- Participation need not be at the decision-making meeting but must occur before final action.

8

## PUBLIC PARTICIPATION GUIDELINES

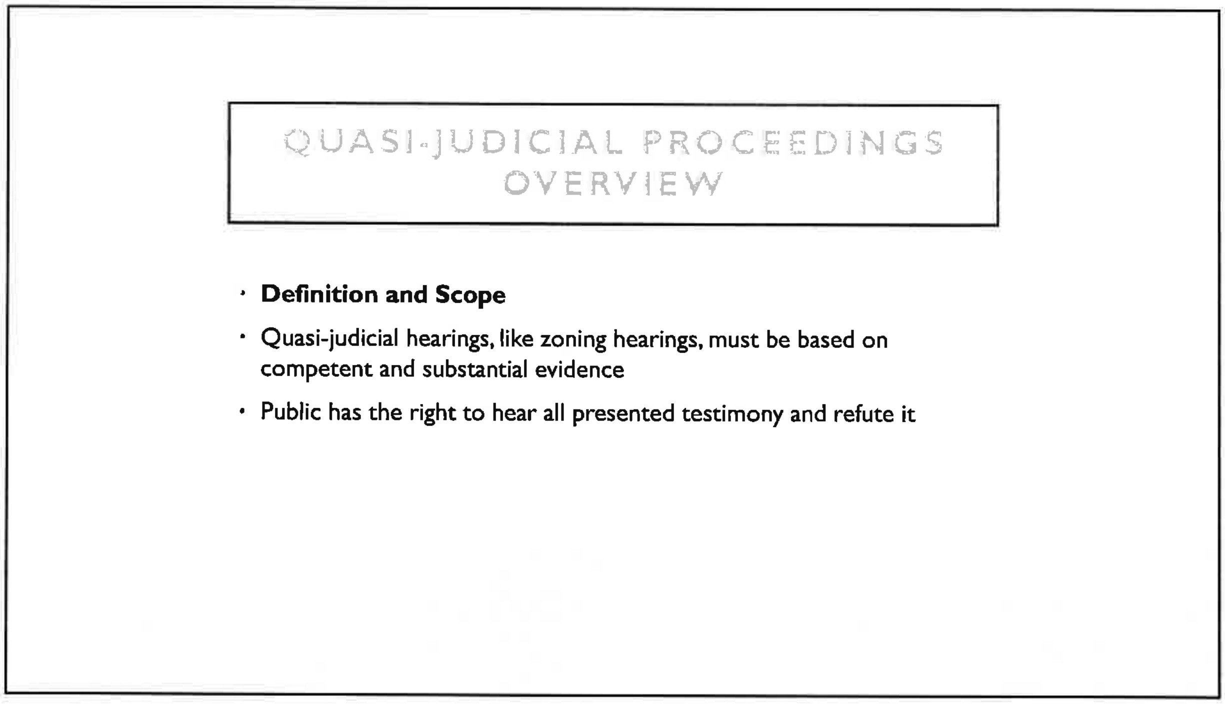
- Public has the right to hear all board-related comments.
- Avoid side conversations, sidebars, private notes, or messages during meetings.
- Time limits on comments are permitted but should not limit meaningful participation.

9

## SCOPE OF COVERAGE

- **Who is Covered?**
- Elected bodies, advisory boards, and any individuals delegated authority to act on behalf of the board.
- Includes council members, councilmembers-elect, and advisory board members.

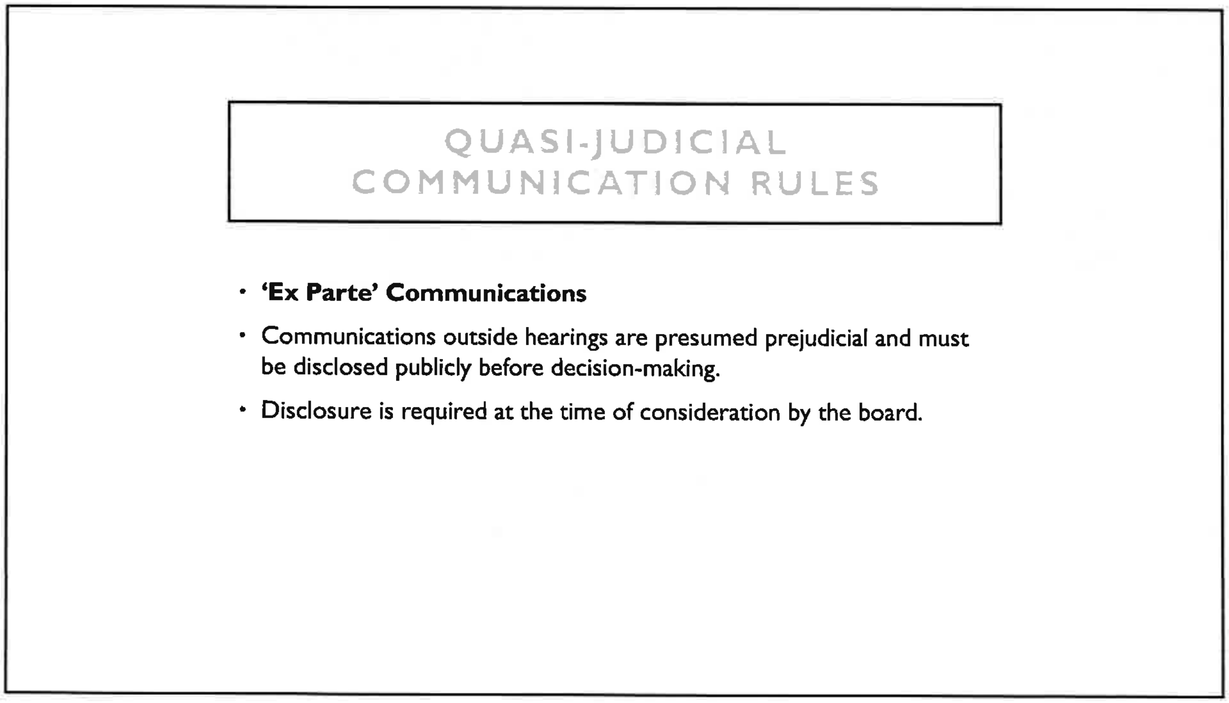
10



## QUASI-JUDICIAL PROCEEDINGS OVERVIEW

- **Definition and Scope**
- Quasi-judicial hearings, like zoning hearings, must be based on competent and substantial evidence
- Public has the right to hear all presented testimony and refute it

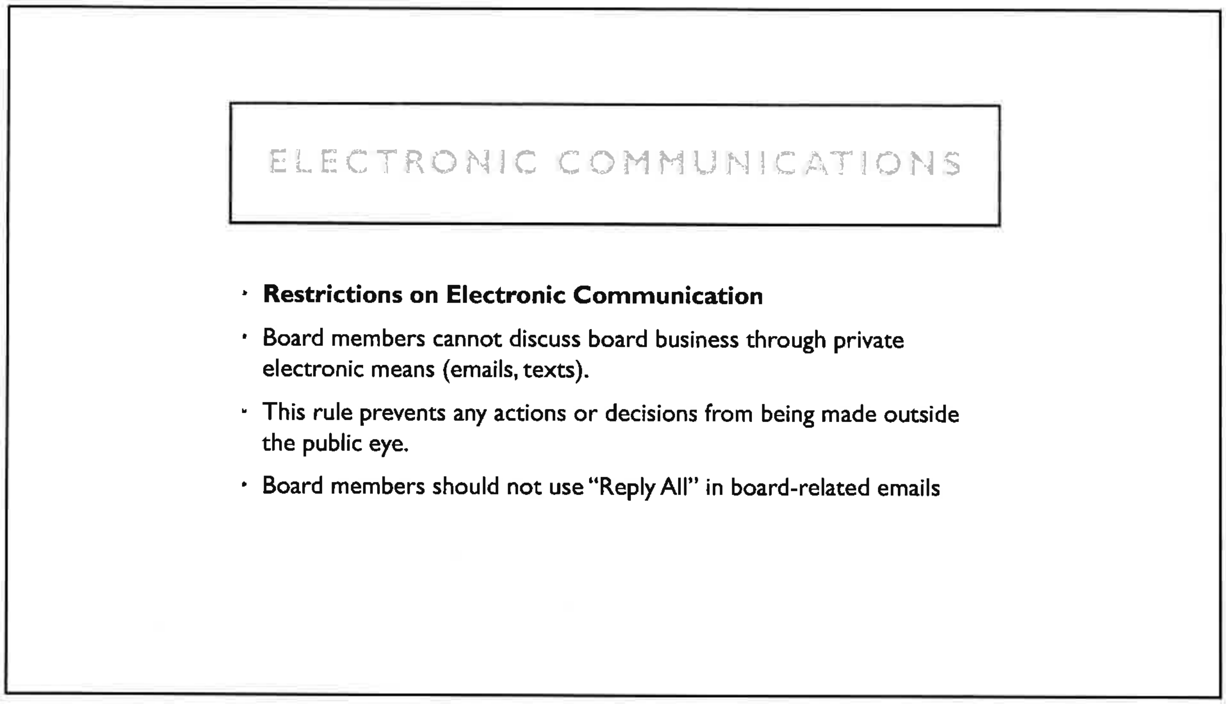
11



## QUASI-JUDICIAL COMMUNICATION RULES

- **'Ex Parte' Communications**
- Communications outside hearings are presumed prejudicial and must be disclosed publicly before decision-making.
- Disclosure is required at the time of consideration by the board.

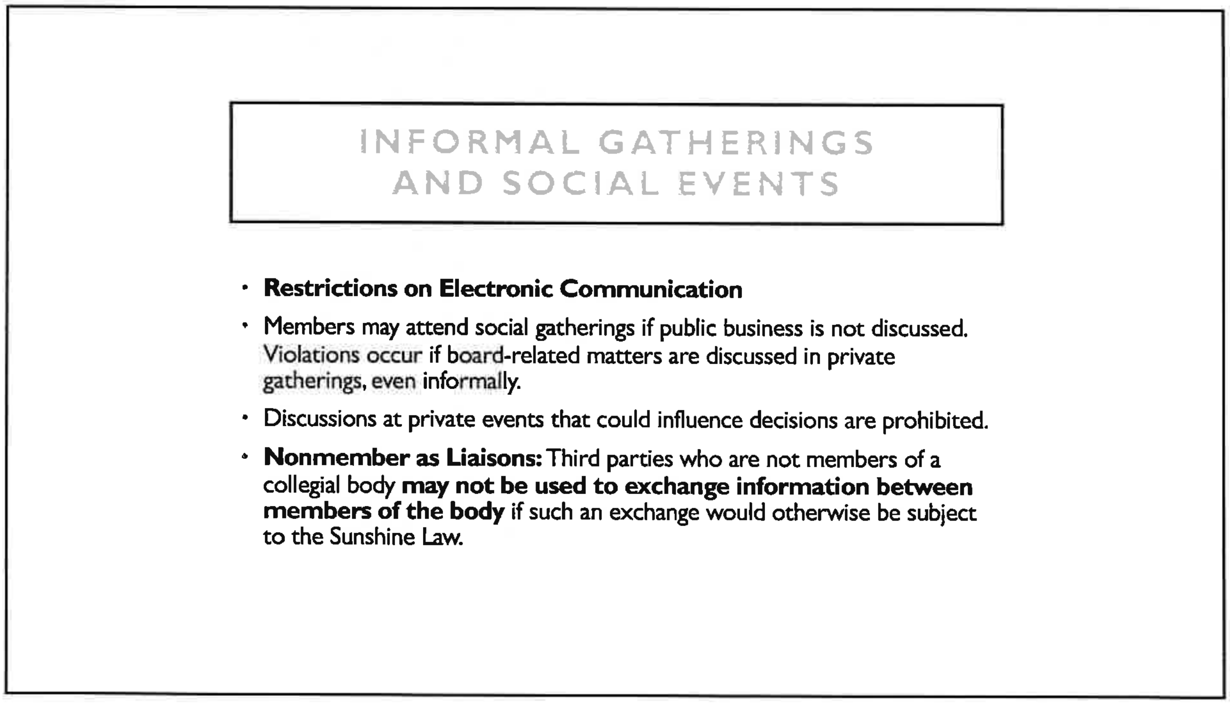
12



## ELECTRONIC COMMUNICATIONS

- **Restrictions on Electronic Communication**
- Board members cannot discuss board business through private electronic means (emails, texts).
- This rule prevents any actions or decisions from being made outside the public eye.
- Board members should not use "Reply All" in board-related emails

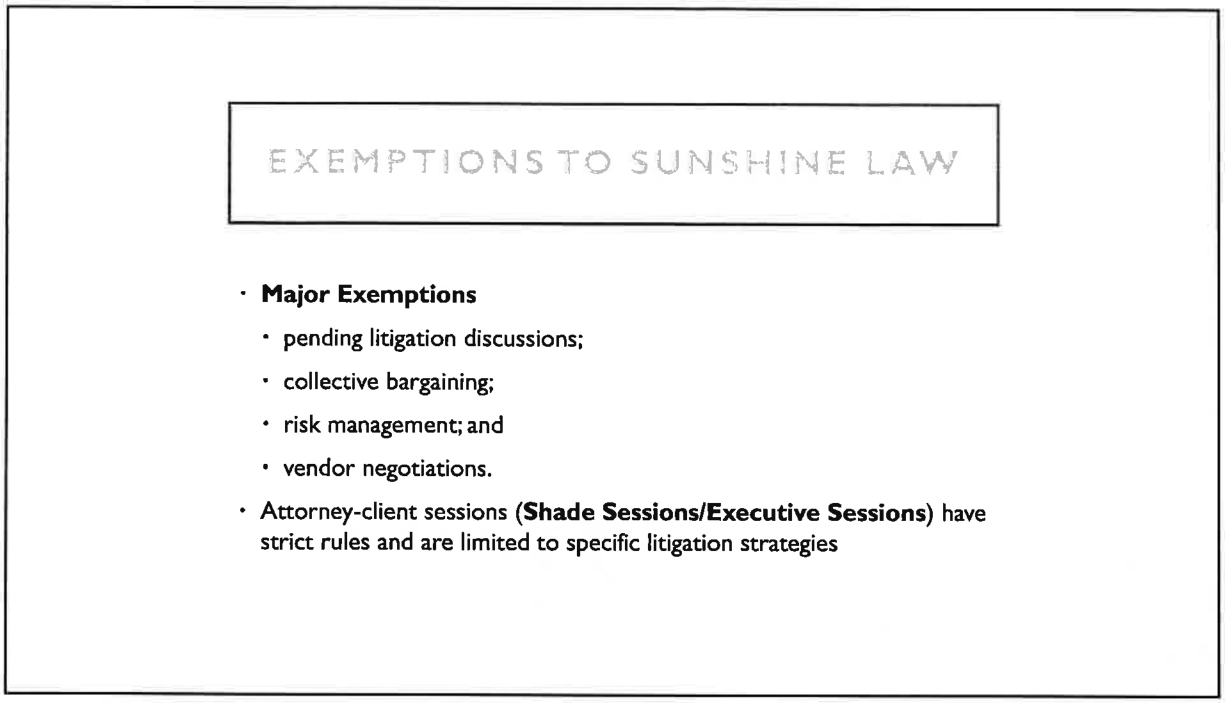
13



## INFORMAL GATHERINGS AND SOCIAL EVENTS

- **Restrictions on Electronic Communication**
- Members may attend social gatherings if public business is not discussed. Violations occur if board-related matters are discussed in private gatherings, even informally.
- Discussions at private events that could influence decisions are prohibited.
- **Nonmember as Liaisons:** Third parties who are not members of a collegial body **may not be used to exchange information between members of the body** if such an exchange would otherwise be subject to the Sunshine Law.

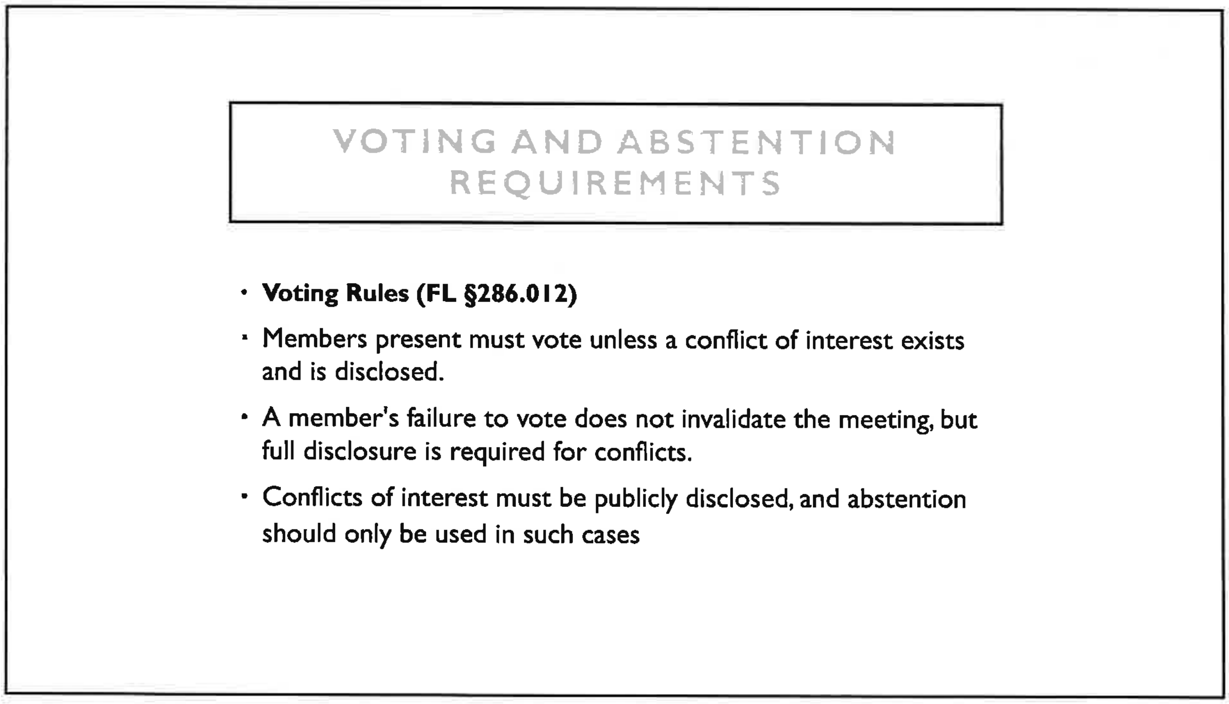
14



## EXEMPTIONS TO SUNSHINE LAW

- **Major Exemptions**
  - pending litigation discussions;
  - collective bargaining;
  - risk management; and
  - vendor negotiations.
- Attorney-client sessions (**Shade Sessions/Executive Sessions**) have strict rules and are limited to specific litigation strategies

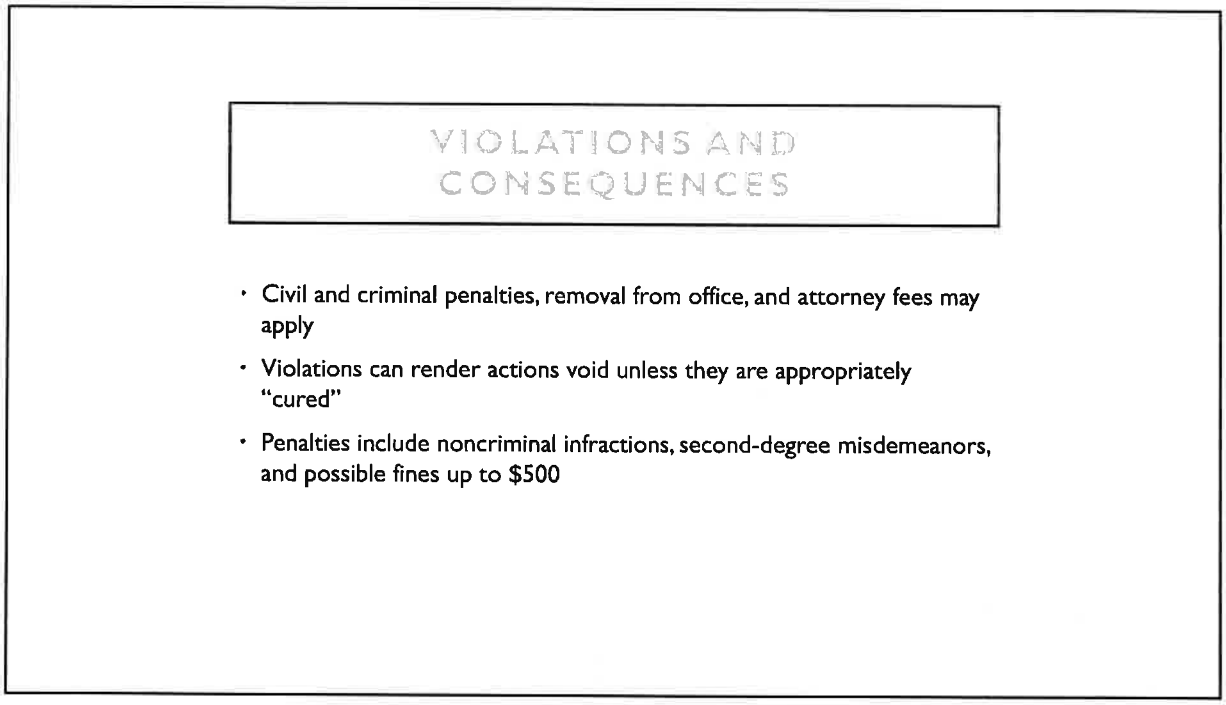
15



## VOTING AND ABSTENTION REQUIREMENTS

- **Voting Rules (FL §286.012)**
- Members present must vote unless a conflict of interest exists and is disclosed.
- A member's failure to vote does not invalidate the meeting, but full disclosure is required for conflicts.
- Conflicts of interest must be publicly disclosed, and abstention should only be used in such cases

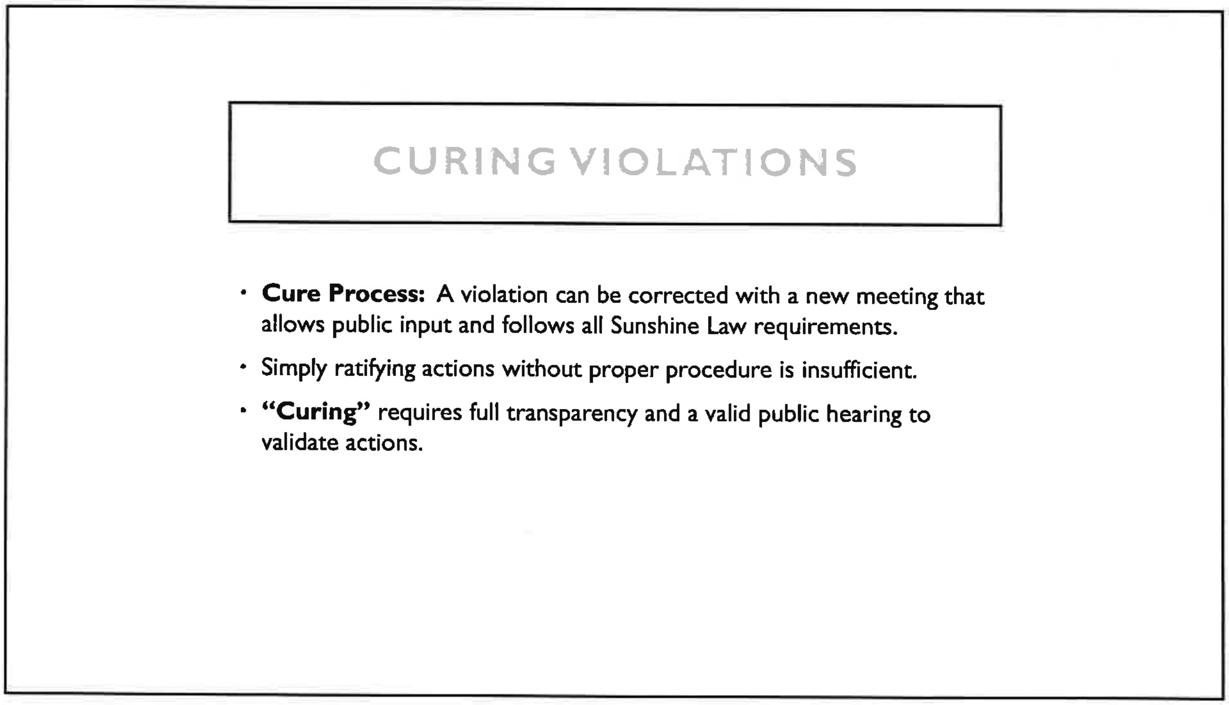
16



## VIOLATIONS AND CONSEQUENCES

- Civil and criminal penalties, removal from office, and attorney fees may apply
- Violations can render actions void unless they are appropriately "cured"
- Penalties include noncriminal infractions, second-degree misdemeanors, and possible fines up to $500

17



## CURING VIOLATIONS

- **Cure Process:** A violation can be corrected with a new meeting that allows public input and follows all Sunshine Law requirements.
- Simply ratifying actions without proper procedure is insufficient.
- **"Curing"** requires full transparency and a valid public hearing to validate actions.

18

## CASE EXAMPLES OF VIOLATIONS

- *City of Bradenton Beach v. Metz* (2019): Informal meetings involving planning and zoning violated the law.
- *State v. Foster* (2005):A private meeting with multiple commissioners was deemed a violation due to "common facilitator" issues.
- Escambia County Commission Chairman – **sentenced to jail** for a Sunshine Law violation; served 38 days of a 60-day sentence

19

TG Law

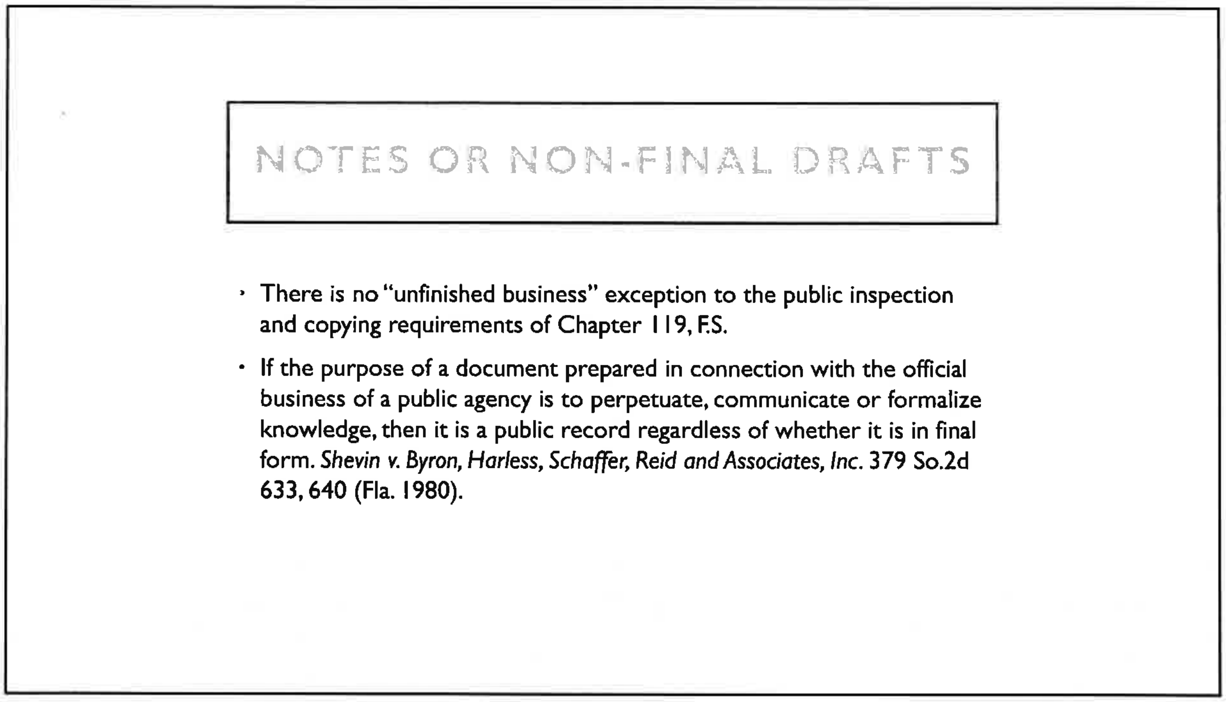
TOWN OF OCEAN BREEZE, FLORIDA

Incorporated 1960

## FLORIDA PUBLIC RECORDS LAW CHAPTER 119, F.S.

**Section 119.11 (11), F.S.**: "Public records" means all documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or other material, regardless of the physical form, characteristics, or means of transmission, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency.

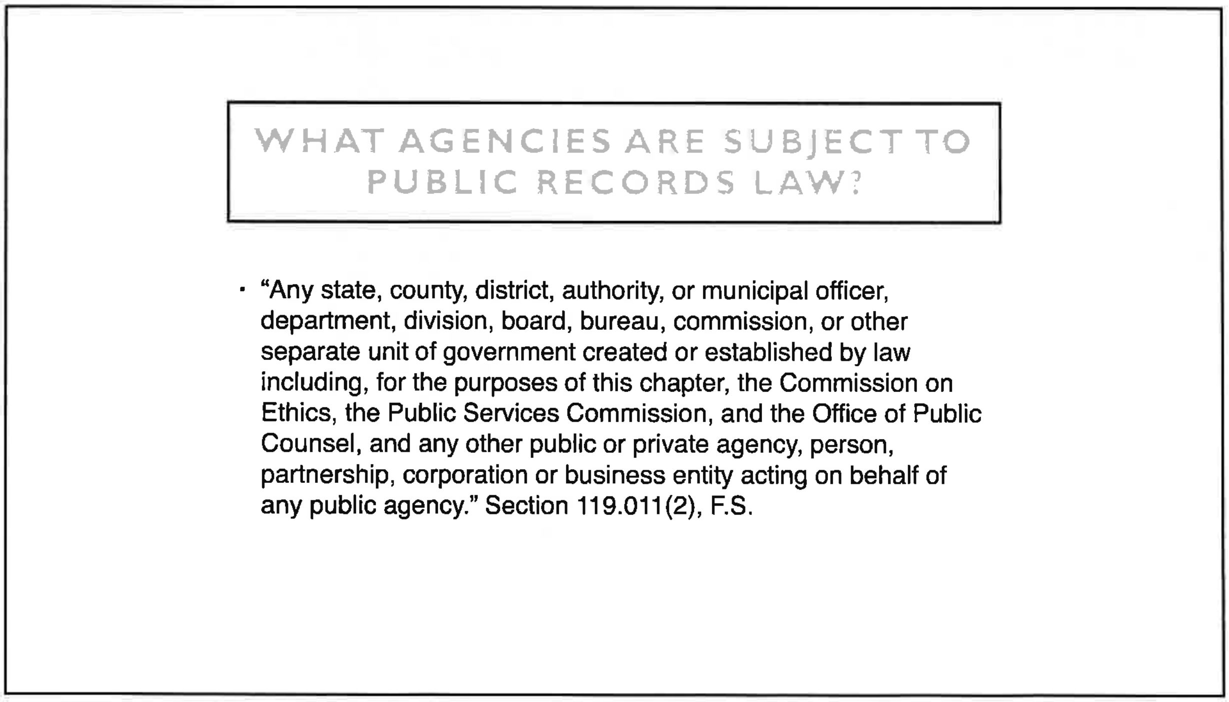
20



## NOTES OR NON-FINAL DRAFTS

- There is no "unfinished business" exception to the public inspection and copying requirements of Chapter 119, F.S.
- If the purpose of a document prepared in connection with the official business of a public agency is to perpetuate, communicate or formalize knowledge, then it is a public record regardless of whether it is in final form. *Shevin v. Byron, Harless, Schaffer, Reid and Associates, Inc.* 379 So.2d 633, 640 (Fla. 1980).

21



## WHAT AGENCIES ARE SUBJECT TO PUBLIC RECORDS LAW?

- "Any state, county, district, authority, or municipal officer, department, division, board, bureau, commission, or other separate unit of government created or established by law including, for the purposes of this chapter, the Commission on Ethics, the Public Services Commission, and the Office of Public Counsel, and any other public or private agency, person, partnership, corporation or business entity acting on behalf of any public agency." Section 119.011(2), F.S.

22

## COMPUTER RECORDS AND EMAIL

- Information stored in a public agency's computer "is as much a public record as a written page in a book or tabulation in a file stored in a filing cabinet." *Seigle v. Barry*, 422 So.2d 63, 65 (Fla. 4th D.C.A. 1982).
- Email messages made or received by agency employees in connection with official business are public records and subject to disclosure in the absence of a statutory exemption from public inspection. AGO. 96-34 (1996).
- ***EXCEPTION*** - Private emails stored in government computers do not automatically become a public record simply by virtue of that storage. *State v. City of Clearwater*, 863 So.2d 149 (Fla. 2003).

23

## TRANSITORY MESSAGES

- Transitory messages are messages of short-term value based upon the content or purpose of the message, not the format used to transmit it (i.e., reminders, event notices, etc.)
- Transitory messages are not intended to formalize or perpetuate knowledge, do not set policy, establish guidelines, confirm a transaction or act as a receipt.
- Retain until obsolete, superseded or administrative value is lost.

24

## WHO RESPONDS TO PUBLIC RECORDS REQUESTS?

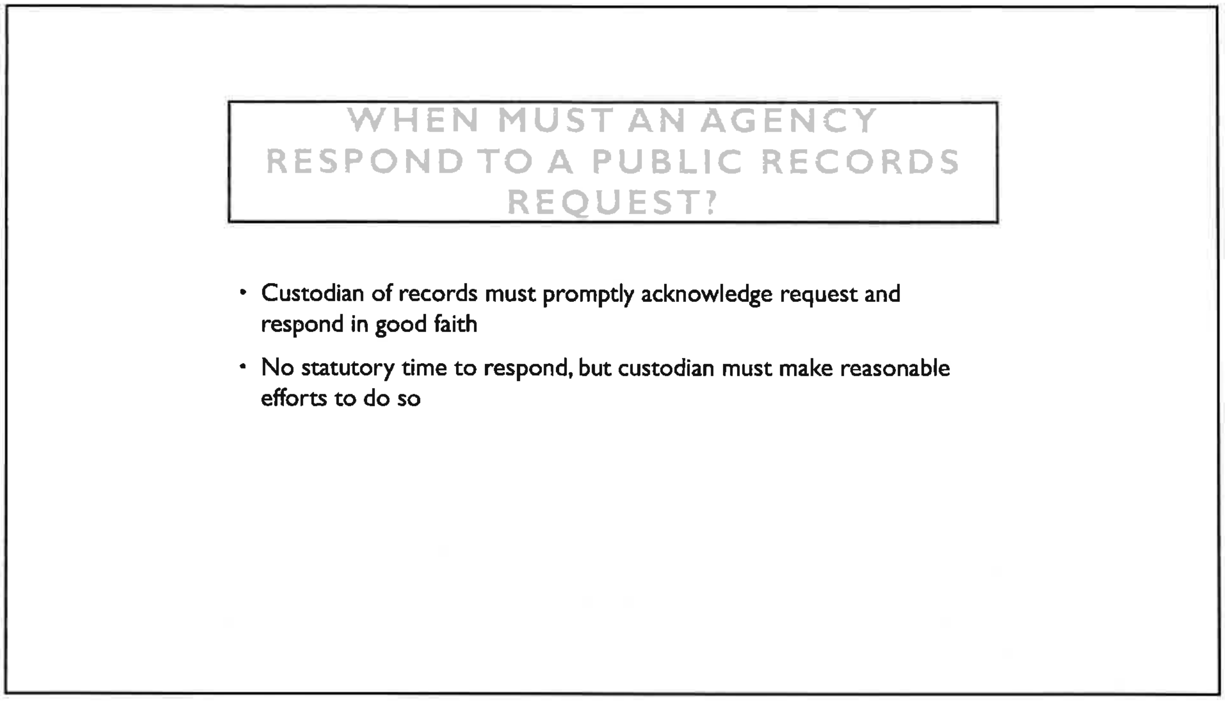
- "Custodian of public records" mean "the elected or appointed state, county or municipal officer charged with the responsibility of maintaining the office having public records, or his or her designee." Section 119.011(5), F.S.
- In Ocean Breeze, Public Records Requests are routed through the City Clerk's Office

25

## WHO IS AUTHORIZED TO INSPECT PUBLIC RECORDS?

- **ANYONE**! Section 119.01, F.S.
- No "legitimate need" or "special purpose" requirement. *See State ex rel. Davis v. McMillan*, 38 So.2d 666 (Fla. 1905).

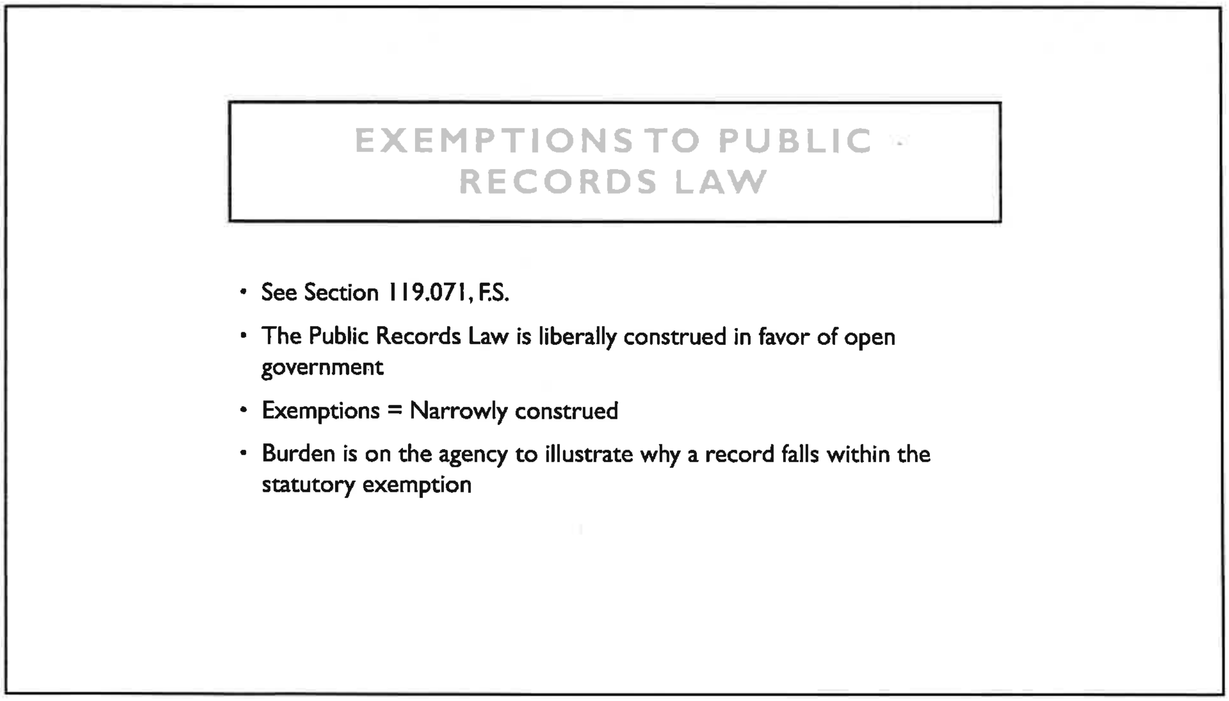
26



## WHEN MUST AN AGENCY RESPOND TO A PUBLIC RECORDS REQUEST?

- Custodian of records must promptly acknowledge request and respond in good faith
- No statutory time to respond, but custodian must make reasonable efforts to do so

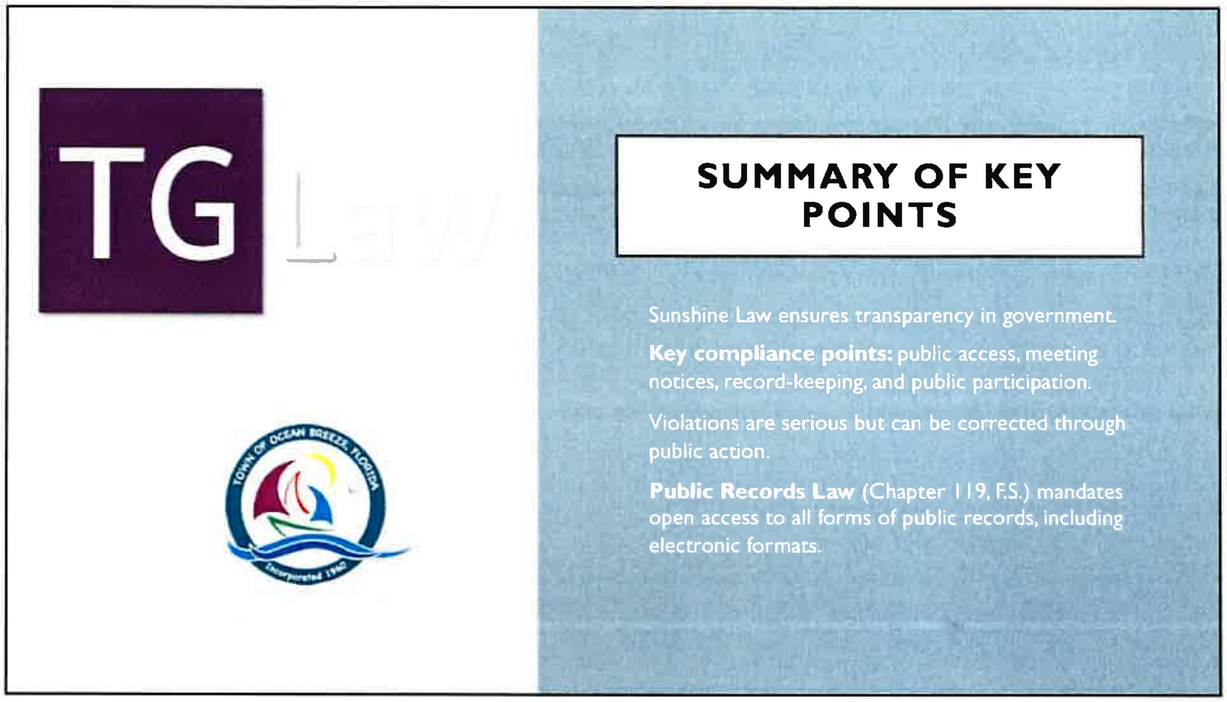
27



## EXEMPTIONS TO PUBLIC RECORDS LAW

- See Section 119.071, F.S.
- The Public Records Law is liberally construed in favor of open government
- Exemptions = Narrowly construed
- Burden is on the agency to illustrate why a record falls within the statutory exemption

28


TG Law
TOWN OF OCEAN BREEZE, FLORIDA
Incorporated 1960

## SUMMARY OF KEY POINTS

Sunshine Law ensures transparency in government.

**Key compliance points:** public access, meeting notices, record-keeping, and public participation.

Violations are serious but can be corrected through public action.

**Public Records Law** (Chapter 119, F.S.) mandates open access to all forms of public records, including electronic formats.

29

# GENERAL INFORMATION ITEMS

**The attached items (i.e.: correspondence, emails, reports, etc.) are provided as general information and are not necessarily subject to discussion during this meeting unless Council Members or the Mayor wish to do so.**

A. Florida Department of Revenue 2024 TRIM certification letter

B. Council Member Gina Kent's resignation

C. Council Member Docherty's IEMO II Certificate of Completion

A.

FLORIDA

**Florida Department of Revenue**
*Property Tax Oversight*

**Jim Zingale**
Executive Director

5050 West Tennessee Street, Tallahassee, FL 32399
floridarevenue.com

December 2, 2024

Karen Ostrand, Mayor
Town of Ocean Breeze
Post Office Box 1025
Jensen Beach, FL 34958

RE: Truth in Millage (TRIM) Certification

Dear Ms. Ostrand:

The Department of Revenue (Department) has reviewed the millage certification documents submitted by your taxing authority. The Department found no violation of the certification requirements in subsections 200.065(1)-(4), (6)-(12), (14), and (15), Florida Statutes (F.S.), and therefore accepts the certification.

The Department also reviewed the maximum millage levy calculation final disclosure documents submitted by your taxing authority. The review included millage levying process documents and documents relating to the total taxes levied by your principal taxing authority, dependent special districts and municipal service taxing units (for counties). Based on the review of these documents, the Department determined that your taxing authority is in compliance with the requirements of maximum total taxes levied, and thus the maximum millage levy requirements of section 200.065(5), F.S.

Sincerely,

Rene Lewis

Rene Lewis, Program Director
Property Tax Oversight

GS/#53.04

B.

## MEMORANDUM

TO: FILE

FROM: KIM STANTON, TOWN CLERK

SUBJECT: GINA KENT, RESIGNATION

DATE: November 13, 2024

---

The purpose of this memorandum is to document that Council Member Gina Kent submitted her resignation from the Town Council effective November 13, 2024.

FLC UNIVERSITY

C.

November 8, 2024

Councilmember Kevin Docherty
Town of Ocean Breeze
PO Box 1025
Jensen Beach, FL 34958-1025

Dear Councilmember Docherty,

On behalf of the Florida League of Cities, I am pleased to award this certificate to you for the completion of the Institute for Elected Municipal Officials II in Altamonte Springs held on October 25-26, 2024.

It is our sincere hope that you found the program and challenging and worthwhile. We encourage you take advantage of other training opportunities through FLC University and recommend our trainings to your colleagues. As a graduate of IEMO I and IEMO II you will now be invited to attend our Leadership Class. This course is invitation only, so keep an eye out for a personalized email from us with more information on the course and the registration link!

We strongly believe that your attendance at the Institute is indicative of your continued commitment to improving the quality of municipal government in Florida. If we may be of assistance in the future, please do not hesitate to call upon us.

Sincerely,

Lynn S. Tipton

Lynn S. Tipton
Director, FLC University
Florida League of Cities

FLC UNIVERSITY

# IEMO II

## Certificate of Completion

October 25-26, 2024 • Altamonte Springs, FL

*Presented to*

**Kevin Docherty**

Councilmember

*Town of Ocean Breeze*

FLC
FLORIDA LEAGUE OF CITIES